Part No. 320657-A
September 2005

4655 Great America Parkway
Santa Clara, CA 95054

Nortel WLAN Security Switch 2300 Series Configuration Guide

Release 4.0



NORTEL

Copyright © Nortel Networks Limited 2005. All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Trademarks

*Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

*Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

USA requirements only

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

Nortel Inc. software license agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1.Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel or certify its destruction. Nortel may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel to include additional or different terms, Customer agrees to abide by such terms provided by Nortel with respect to such third party software.

2.Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3.Limitation of Remedies. IN NO EVENT SHALL Nortel OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE,

OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF Nortel NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4.General

a)If Customer is the United States Government, the following paragraph shall apply: All Nortel Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b)Customer may terminate the license at any time. Nortel may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel or certify its destruction.

c)Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d)Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e)The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel.

f)This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Legal Information

This section includes the following legal information:

- "Limited Product Warranty" on page 4
- "Software License Agreement" on page 6
- "SSH Source Code Statement" on page 8
- "OpenSSL Project License Statements" on page 9
- "Trademarks and Service Marks" on page 9

Limited Product Warranty

The following sections describe the Nortel standard Product Warranty for End Users.

Products

WLAN—Wireless Security Switch (23x0) Family

WLAN—Access Points (2330) Family

Limited Warranty

Nortel standard warranty for hardware is one (1) year. Nortel warrants software materials to be defect free for 90 Days from time of purchase. Nortel requires purchasing the software subscription if a customer would like to receive new WLAN—Wireless Security Switch (23x0), Nortel WLAN — Management System software. This limited warranty extends only to you the original purchaser of the Product.

Exclusive Remedy

Your sole remedy under the limited warranty described above is, at Nortel's sole option and expense, the repair or replacement of the non-conforming Product or refund of the purchase price of the non-conforming Products. Nortel's obligation under this limited warranty is subject to compliance with Nortel's then-current Return Material Authorization ("RMA") procedures. All replaced Products will become the property of Nortel. Exchange Products not returned to Nortel will be invoiced at full Product list prices. Replacement Products may be new, reconditioned or contain refurbished materials. In connection with any warranty services hereunder, Nortel may in its sole discretion modify the Product at no cost to you to improve its reliability or performance.

Warranty Claim Procedures

Should a Product fail to conform to the limited warranty during the applicable warranty period as described above, Nortel must be notified during the applicable warranty period in order to have any obligation under the limited warranty.

The End Customer or their designated reseller must obtain a Return Material Authorization number (RMA number) from Nortel for the non-conforming Product and the non-conforming Product must be returned to Nortel according to the then-current RMA procedures. The End Customer or their designated reseller is responsible to ensure that the shipments are insured, with the transportation charges prepaid and that the RMA number is clearly marked on the outside of the package. Nortel will not accept collect shipments or those returned without an RMA number clearly visible on the outside of the package.

Exclusions and Restrictions

Nortel shall not be responsible for any software, firmware, information or memory data contained in, stored on or integrated with any Product returned to Nortel pursuant to any warranty or repair.

Upon return of repaired or replaced Products by Nortel, the warranty with respect to such Products will continue for the remaining unexpired warranty or sixty (60) days, whichever is longer. Nortel may provide out-of-warranty repair for the Products at its then-prevailing repair rates.

The limited warranty for the Product does not apply if, in the judgment of Nortel, the Product fails due to damage from shipment, handling, storage, accident, abuse or misuse, or it has been used or maintained in a manner not conforming to Product manual instructions, has been modified in any way, or has had any Serial Number removed or defaced. Repair by anyone other than Nortel or an approved agent will void this warranty.

EXCEPT FOR ANY EXPRESS LIMITED WARRANTIES FROM Nortel SET FORTH ABOVE, THE PRODUCT IS PROVIDED "AS IS", AND Nortel AND ITS SUPPLIERS MAKE NO WARRANTY, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, WITH RESPECT TO PRODUCT OR ANY PART THEREOF, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR THOSE ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. Nortel'S SUPPLIERS MAKE NO DIRECT WARRANTY OF ANY KIND TO END CUSTOMER FOR THE LICENSED MATERIALS. NEITHER Nortel NOR ANY OF ITS SUPPLIERS WARRANT THAT THE LICENSED

MATERIALS OR ANY PART THEREOF WILL MEET END CUSTOMER'S REQUIREMENTS OR BE UNINTERRUPTED, OR ERROR-FREE, OR THAT ANY ERRORS IN THE PRODUCT WILL BE CORRECTED. SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO END CUSTOMER. THIS LIMITED WARRANTY GIVES END CUSTOMER SPECIFIC LEGAL RIGHTS. END CUSTOMER MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM STATE/JURISDICTION TO STATE/ JURISDICTION.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL Nortel OR ITS SUPPLIERS BE LIABLE FOR THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF PROFITS, OR FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, PUNITIVE OR INDIRECT DAMAGES (OR DIRECT DAMAGES IN THE CASE OF Nortel'S SUPPLIERS) ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, TORT (INCLUDING WITHOUT LIMITATION NEGLIGENCE), STRICT LIABILITY OR OTHERWISE ARISING OUT OF OR RELATED TO THE PRODUCT OR ANY USE OR INABILITY TO USE THE PRODUCT. Nortel'S TOTAL LIABILITY ARISING OUT OF OR RELATED TO THE PRODUCT, OR USE OR INABILITY TO USE THE PRODUCT, WHETHER IN CONTRACT, TORT (INCLUDING WITHOUT LIMITATION NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THE LIMITATIONS SET FORTH IN THIS SECTION SHALL APPLY EVEN IF Nortel AND/OR ITS SUPPLIERS ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. Nortel NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

Software License Agreement

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THE SOFTWARE AND ASSOCIATED DOCUMENTATION THAT IS PROVIDED WITH THIS AGREEMENT ("SOFTWARE," "DOCUMENTATION," AND COLLECTIVELY, "LICENSED MATERIALS").

BY USING ANY LICENSED MATERIALS, YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT AND YOU WILL BE CONSENTING TO BE BOUND BY THEM. IF YOU DO NOT ACCEPT THESE TERMS AND CONDITIONS, DO NOT USE THE LICENSED MATERIALS AND RETURN THE LICENSED MATERIALS AND ANY EQUIPMENT PROVIDED BY Nortel IN CONNECTION THEREWITH ("EQUIPMENT") UNUSED IN THE ORIGINAL SHIPPING CONTAINER TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Software may be provided by Nortel on a standalone basis ("Standalone Software") or it may be provided embedded in Equipment ("Embedded Software").

1. License.

(a) Subject to the terms and conditions of this Agreement, Nortel ("Nortel"), grants to you ("Licensee") a limited, non-exclusive, non-transferable license, without the right to sublicense: (i) to install and use the Standalone Software, in object code format only, on computer hardware for which all corresponding license fees have been paid; (ii) use one (1) copy of the Embedded Software, in object code format only, solely as embedded in Equipment, each solely in accordance with the Documentation for Licensee's internal business purposes.

(b) The license set forth above does not include any rights to and Licensee shall not (i) reproduce (except as set forth in Section 1(c)), modify, translate or create any derivative work of all or any portion of the Licensed Materials or Equipment, (ii) sell, rent, lease, loan, provide, distribute or otherwise transfer all or any portion of the Licensed Materials (except as set forth in Section 1(f)), (iii) reverse engineer, reverse assemble or otherwise attempt to gain access to the source code of all or any portion of the Licensed Materials or Equipment, (iv) use the Licensed Materials for third-party training, commercial time-sharing or service bureau use, (v) remove, alter, cover or obfuscate any copyright notices, trademark notices or other proprietary rights notices placed or embedded on or in the Licensed Materials or Equipment, (vi) use any component of the Software or Equipment other than solely in conjunction with operation of the Software and as applicable, Equipment, (vii) unbundle any component of the Software or Equipment, (viii) use any component of the Software for the development of or in conjunction with any software application intended for resale that employs any such component, (ix) use the Licensed Materials or Equipment in life support systems, human implantation, nuclear facilities or systems or any other application where failure could lead to a loss of life or catastrophic property damage, or (x) cause or permit any third party to do any of the foregoing.

If Licensee is a European Union resident, Licensee acknowledges that information necessary to achieve interoperability of the Software with other programs is available upon request.

(c) Licensee may make a single copy of the Standalone Software and Documentation solely for its back-up purposes; provided that any such copy is the exclusive property of Nortel and its suppliers and includes all copyright and other intellectual property right notices that appear on the original.

(d) Nortel may provide updates, corrections, enhancements, modifications or bug fixes for the Licensed Materials ("Updates") to Licensee. Any such Update shall be deemed part of the Licensed Materials and subject to the license and all other terms and conditions hereunder.

(e) Nortel shall have the right to inspect and audit Licensee's use, deployment, and exploitation of the Licensed Materials for compliance with the terms and conditions of this Agreement.

(f) Licensee shall have the right to transfer the Embedded Software as embedded in Equipment in connection with a transfer of all of Licensee's right, title and interest in such Equipment to a third party; provided, that, Licensee transfers the Embedded Software and any copies thereof subject to the terms and conditions of this Agreement and such third party agrees in writing to be bound by all the terms and conditions of this Agreement.

(g) Notwithstanding anything to the contrary herein, certain portions of the Software are licensed under and Licensee's use of such portions are only subject to the GNU General Public License version 2. If Licensee or any third party sends a request in writing to Nortel at 110 Nortech Parkway, San Jose CA 95134, ATTN: Contracts Administration, Nortel will provide a complete machine-readable copy of the source code of such portions for a nominal cost to cover Nortel's cost in physically providing such code.

2. Ownership. Nortel or its suppliers own and shall retain all right, title and interest (including without limitation all intellectual property rights), in and to the Licensed Materials and any Update, whether or not made by Nortel. Licensee acknowledges that the licenses granted under this Agreement do not provide Licensee with title to or ownership of the Licensed Materials, but only a right of limited use under the terms and conditions of this Agreement. Except as expressly set forth in Section 1, Nortel reserves all rights and grants Licensee no licenses of any kind hereunder. All information or feedback provided by Licensee to Nortel with respect to the Software or Equipment shall be Nortel's property and deemed confidential information of Nortel.

3. Confidentiality. Licensee agrees that the Licensed Materials contain confidential information, including trade secrets, know-how, and information pertaining to the technical structure or performance of the Software, that is the exclusive property of Nortel as between Licensee and Nortel. In addition, Nortel's confidential information includes any confidential or trade secret information related to the Licensed Materials. During the period this Agreement is in effect and at all times thereafter, Licensee shall maintain Nortel's confidential information in confidence and use the same degree of care, but in no event less than reasonable care, to avoid disclosure of Nortel's confidential information as it uses with respect to its own confidential and proprietary information of similar type and importance. Licensee agrees to only disclose Nortel's confidential information to its directors, officers and employees who have a bona fide need to know solely to exercise Licensee's rights under this Agreement and to only use Nortel's confidential information incidentally in the customary operation of the Software and Equipment. Licensee shall not sell, license, sublicense, publish, display, distribute, disclose or otherwise make available Nortel's confidential information to any third party nor use such information except as authorized by this Agreement. Licensee agrees to immediately notify Nortel of the unauthorized disclosure or use of the Licensed Materials and to assist Nortel in remedying such unauthorized use or disclosure. It is further understood and agreed that any breach of this Section 3 or Section 1(b) is a material breach of this Agreement and any such breach would cause irreparable harm to Nortel and its suppliers, entitling Nortel or its suppliers to injunctive relief in addition to all other remedies available at law.

4. Limited Warranty & Disclaimer. Any limited warranty for the Licensed Materials and Nortel's sole and exclusivity liability thereunder is as set forth in Nortel's standard warranty documentation. In addition, any limited warranty for the Software does not apply to any component of the Software but only to the Software as a whole. EXCEPT FOR ANY EXPRESS LIMITED WARRANTIES FROM Nortel IN SUCH DOCUMENTATION, THE LICENSED MATERIALS ARE PROVIDED "AS IS", AND Nortel AND ITS SUPPLIERS MAKE NO WARRANTY, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, WITH RESPECT TO LICENSED MATERIALS OR ANY PART THEREOF, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THOSE ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. Nortel'S SUPPLIERS MAKE NO DIRECT WARRANTY OF ANY KIND TO LICENSEE FOR THE LICENSED MATERIALS. NEITHER Nortel NOR ANY OF ITS SUPPLIERS WARRANT THAT THE LICENSED MATERIALS OR ANY PART THEREOF WILL MEET LICENSEE'S REQUIREMENTS OR BE UNINTERRUPTED, OR ERROR-FREE, OR THAT ANY ERRORS IN THE LICENSED MATERIALS WILL BE CORRECTED. SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO LICENSEE. THIS LIMITED WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS. LICENSEE MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM STATE/JURISDICTION TO STATE/JURISDICTION.

5. Term and Termination. This Agreement is effective until terminated. License may terminate this Agreement at any time by destroying all copies of the Software. This Agreement and all licenses granted hereunder will terminate immediately without notice from Nortel if Licensee fails to comply with any provision of this Agreement. Upon any termination, Licensee must destroy all copies of the Licensed Materials. Sections 1(b), 2, 3, 4(b), 5, 6, 7, 8, 9 and 10 shall survive any termination of this Agreement.

6. Export. The Software is specifically subject to U.S. Export Administration Regulations. Licensee agrees to strictly comply with all export, re-export and import restrictions and regulations of the Department of Commerce or other agency or authority of the United States or other applicable countries, and not to transfer, or authorize the transfer of, directly or indirectly, the Software or any direct product thereof to a prohibited country or otherwise in violation of any such restrictions or regulations. Licensee's failure to comply with this Section is a material breach of this Agreement. Licensee acknowledges that Licensee is not a national of Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria or a party listed in the U.S. Table of Denial Orders or U.S. Treasury Department List of Specially Designated Nationals.

7. Government Restricted Rights. As defined in FAR section 2.101, DFAR section 252.227-7014(a)(1) and DFAR section 252.227-7014(a)(5) or otherwise, the Software provided in connection with this Agreement are "commercial items," "commercial computer software" and/or "commercial computer software documentation." Consistent with DFAR section 227.7202, FAR section 12.212 and other sections, any use, modification, reproduction, release, performance, display, disclosure or distribution thereof by or for the U.S. Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Any technical data provided that is not covered by the above provisions shall be deemed "technical data-commercial items" pursuant to DFAR section 227.7015(a). Any use, modification, reproduction, release, performance, display or disclosure of such technical data shall be governed by the terms of DFAR section 227.7015(b).

8. Limitation of Liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL Nortel OR ITS SUPPLIERS BE LIABLE FOR THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF PROFITS, OR FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, PUNITIVE OR INDIRECT DAMAGES (OR DIRECT DAMAGES IN THE CASE OF Nortel'S SUPPLIERS) ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, TORT (INCLUDING WITHOUT LIMITATION NEGLIGENCE), STRICT LIABILITY OR OTHERWISE ARISING OUT OF OR UNDER THIS AGREEMENT OR ANY USE OR INABILITY TO USE THE LICENSED MATERIALS OR EQUIPMENT, OR FOR BREACH OF THIS AGREEMENT. Nortel'S TOTAL LIABILITY ARISING OUT OF OR UNDER THIS AGREEMENT, OR USE OR INABILITY TO USE THE LICENSED MATERIALS OR EQUIPMENT, OR FOR BREACH OF THIS AGREEMENT, WHETHER IN CONTRACT, TORT (INCLUDING WITHOUT LIMITATION NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID FOR THE SOFTWARE (FOR THE STANDALONE SOFTWARE) AND THE PRICE PAID FOR THE EQUIPMENT (FOR THE EMBEDDED SOFTWARE AND EQUIPMENT). THE LIMITATIONS SET FORTH IN THIS SECTION SHALL APPLY EVEN IF Nortel AND/OR ITS SUPPLIERS ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

9. Third Party Beneficiaries. Nortel's suppliers are intended third party beneficiaries of this Agreement. The terms and conditions herein are made expressly for the benefit of and are enforceable by Nortel's suppliers; provided, however, that Nortel's suppliers are not in any contractual relationship with Licensee. Nortel's suppliers include without limitation: (a) Hifn, Inc., a Delaware corporation with principal offices at 750 University Avenue, Los Gatos, California; and (b) Wind River Systems, Inc. and its suppliers.

10. General. This Agreement is governed and interpreted in accordance with the laws of the State of California, U.S.A. without reference to conflicts of laws principles and excluding the United Nations Convention on Contracts for the Sale of Goods. The parties consent to the exclusive jurisdiction of, and venue in, Santa Clara County, California, U.S.A. Licensee shall not transfer, assign or delegate this Agreement or any rights or obligations hereunder, whether voluntarily, by operation of law or otherwise, without the prior written consent of Nortel (except as expressly set forth in Section 1(f)). Subject to the foregoing, the terms and conditions of this Agreement shall be binding upon and inure to the benefit of the parties to it and their respective heirs, successors, assigns and legal representatives. This Agreement constitutes the entire agreement between Nortel and Licensee with respect to the subject matter hereof, and merges all prior negotiations and drafts of the parties with regard thereto. No modification of or amendment to this Agreement, nor any waiver of any rights under this Agreement, by Nortel shall be effective unless in writing. If any of the provisions of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable under any applicable statute or rule of law, such provision shall, to that extent, be deemed omitted.

SSH Source Code Statement

C 1995 - 2004 SAFENET, Inc. This software is protected by international copyright laws. All rights reserved. SafeNet is a registered trademark of SAFENET, Inc., in the United States and in certain other jurisdictions. SAFENET and the SAFENET logo are trademarks of SAFENET, Inc., and may be registered in certain jurisdictions. All other names and marks are property of their respective owners.

Copyright (c) 1983, 1990, 1992, 1993, 1995 The Regents of the University of California. All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEAPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

- Markus Friedl
- Theo de Raadt
- Niels Provos
- Dug Song
- Aaron Campbell

o Damien Miller

o Kevin Steves

o Daniel Kouril

o Per Allansson

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEAPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSSL Project License Statements

Copyright (c) 1998-2002 The OpenSSL Project. All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEAPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEAPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Trademarks and Service Marks

Nortel, and the Nortel logo are registered trademarks, and management software is a trademark of Nortel All other trademarks belong to their respective holders.



FCC Statements for WLAN—Security Switches (23xx)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Statements for WLAN—Access Points (2330)

This section includes the following FCC statements for WLAN—Access Points (2330):

- "Class A Statement" on page 10
- "RF Radiation Hazard Warning" on page 10
- "Non-Modification Statement" on page 10
- "Deployment Statement" on page 11

Class A Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

RF Radiation Hazard Warning

To ensure compliance with FCC RF exposure requirements, this device must be installed in a location such that the antenna of the device will be greater than 20 cm (8 in.) from all persons. Using higher gain antennas and types of antennas not covered under the FCC certification of this product is not allowed.

Installers of the radio and end users of the Nortel 2300 Series must adhere to the installation instructions provided in this manual.

Non-Modification Statement

Use only the supplied internal antenna, or external antennas supplied by the manufacturer. Unauthorized antennas, modifications, or attachments could damage the badge and could violate FCC regulations and void the user's authority to operate the equipment.

Note: Refer to the *Nortel 2300 Series Release Notes* for 802.11a external antenna information. Contact Nortel for a list of FCC-approved 802.11a and 802.11b/g external antennas.

Deployment Statement

This product is certified for indoor deployment only. Do not install or use this product outdoors.

Industry Canada Required User Information for WLAN—Access Points (2330)

This device has been designed to operate with antennae having maximum gains of 7.8 dBi (2.4 GHz) and 7.4 dBi (5 GHz).

Antennae having higher gains is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

To ensure compliance with EMC standards applied to the Nortel WLAN—Wireless Security Switches (23x0), shielded twisted pair (STP) 10/100Base-T cabling must be used.

Contents

How to get Help 29

Introducing the Nortel WLAN 2300 System 31

Nortel WLAN 2300 System 31
Documentation 32
Safety and Advisory Notices 33
Text and Syntax Conventions 34

Using the Command-Line Interface 35

CLI Conventions 35
Command Prompts 36
Syntax Notation 37
Text Entry Conventions and Allowed Characters 38
User Wildcards, MAC Address Wildcards, and VLAN Wildcards 39
Port Lists 41
Virtual LAN Identification 42
Command-Line Editing 43
Keyboard Shortcuts 44
History Buffer 45
Tabs 46
Single-Asterisk (*) Wildcard Character 47
Double-Asterisk (**) Wildcard Characters 48
Using CLI Help 49
Understanding Command Descriptions 50

Configuring AAA for Administrative and Local Access 51

Overview of AAA for Administrative and Local Access 51
Before You Start 53
About Administrative Access 54
Access Modes 55
Types of Administrative Access 56
First-Time Configuration using the Console 56
Enabling an Administrator 57

Setting the WSS Switch Enable Password 58
Authenticating at the Console 60
Customizing AAA with “Wildcards” and Groups 61
Setting User Passwords 62
Adding and Clearing Local Users for Administrative Access 63
Configuring Accounting for Administrative Users 63
Displaying the AAA Configuration 65
Saving the Configuration 65
Administrative AAA Configuration Scenarios 66
Local Authentication 67
Local Authentication for Console Users and RADIUS Authentication for Telnet Users 68
Local Override and Backup Local Authentication 69
Authentication When RADIUS Servers Do Not Respond 70

Configuring and Managing Ports and VLANs 71

Configuring and Managing Ports 71
Setting the Port Type 72
WSS 2380 40 AP Software License Upgrade 73
Configuring a Port Name 79
Configuring Interface Preference on a Dual-Interface Gigabit Ethernet Port (WSS-400 only) 80
Configuring Port Operating Parameters 81
Displaying Port Information 84
Configuring Load-Sharing Port Groups 87
Configuring and Managing VLANs 88
Understanding VLANs in Nortel WSS Software 89
Configuring a VLAN 92
Changing Tunneling Affinity 95
Displaying VLAN Information 96
Managing the Layer 2 Forwarding Database 96
Types of Forwarding Database Entries 97
How Entries Enter the Forwarding Database 98
Displaying Forwarding Database Information 99
Adding an Entry to the Forwarding Database 100
Removing Entries from the Forwarding Database 101

Configuring the Aging Timeout Period 102
Port and VLAN Configuration Scenario 102

Configuring and Managing IP Interfaces and Services 107

MTU Support 107
Configuring and Managing IP Interfaces 108
Adding an IP Interface 109
Disabling or Reenabling an IP Interface 112
Removing an IP Interface 113
Displaying IP Interface Information 114
Configuring the System IP Address 114
Designating the System IP Address 115
Displaying the System IP Address 116
Clearing the System IP Address 117
Configuring and Managing IP Routes 117
Displaying IP Routes 119
Adding a Static Route 121
Removing a Static Route 122
Managing the Management Services 122
Managing SSH 123
Managing Telnet 126
Managing HTTPS 128
Configuring and Managing DNS 128
Enabling or Disabling the DNS Client 130
Configuring DNS Servers 131
Configuring a Default Domain Name 132
Displaying DNS Server Information 133
Configuring and Managing Aliases 133
Adding an Alias 134
Removing an Alias 135
Displaying Aliases 136
Configuring and Managing Time Parameters 136
Setting the Time Zone 137
Configuring the Summertime Period 138
Statically Configuring the System Time and Date 139
Displaying the Time and Date 140

Configuring and Managing NTP 141
Adding an NTP Server 142
Removing an NTP Server 143
Changing the NTP Update Interval 144
Resetting the Update Interval to the Default 145
Enabling the NTP Client 146
Displaying NTP Information 147
Managing the ARP Table 147
Displaying ARP Table Entries 148
Adding an ARP Entry 149
Changing the Aging Timeout 150
Pinging Another Device 150
Logging In to a Remote Device 151
Tracing a Route 152
IP Interfaces and Services Configuration Scenario 152

Configuring SNMP 155

Overview 155
Configuring SNMP 155
Setting the System Location and Contact Strings 156
Enabling SNMP Versions 157
Configuring Community Strings (SNMPv1 and SNMPv2c Only) 158
Creating a USM User for SNMPv3 159
Setting SNMP Security 161
Configuring a Notification Profile 162
Configuring a Notification Target 165
Enabling the SNMP Service 167
Displaying SNMP Information 167
Displaying SNMP Version and Status Information 168
Displaying the Configured SNMP Community Strings 169
Displaying USM Settings 170
Displaying Notification Profiles 171
Displaying Notification Targets 172
Displaying SNMP Statistics Counters 173

Configuring and Managing Mobility Domain Roaming 175

About the Mobility Domain Feature 175
Configuring a Mobility Domain 176
Configuring the Seed 177
Configuring Member WSSs on the Seed 178
Configuring a Member 179
Displaying Mobility Domain Status 180
Displaying the Mobility Domain Configuration 181
Clearing a Mobility Domain from a WSS 182
Clearing a Mobility Domain Member from a Seed 183
Monitoring the VLANs and Tunnels in a Mobility Domain 183
Displaying Roaming Stations 184
Displaying Roaming VLANs and Their Affinities 185
Displaying Tunnel Information 186
Understanding the Sessions of Roaming Users 186
Requirements for Roaming to Succeed 187
Effects of Timers on Roaming 188
Monitoring Roaming Sessions 189
Mobility Domain Scenario 189

Configuring User Encryption 191

Configuring WPA 194
WPA Cipher Suites 195
TKIP Countermeasures 198
WPA Authentication Methods 199
WPA Information Element 200
Client Support 201
Configuring WPA 203
Configuring RSN (802.11i) 207
Configuring WEP 209
Setting Static WEP Key Values 211
Assigning Static WEP Keys 212
Encryption Configuration Scenarios 212
Enabling WPA with TKIP 213
Enabling Dynamic WEP in a WPA Network 215

Configuring Encryption for MAC Clients 217

Configuring AP access points 221

AP Overview 221
Country of Operation 223
Directly Connected APs and Distributed APs 224
Service Profiles 240
Radio Profiles 244
Configuring AP access points 247
Specifying the Country of Operation 248
Configuring a Template for Automatic AP Configuration 251
Configuring AP Port Parameters 256
Configuring AP-WSS Security 261
Configuring a Service Profile 265
Configuring a Radio Profile 267
Configuring Radio-Specific Parameters 273
Mapping the Radio Profile to Service Profiles 276
Assigning a Radio Profile and Enabling Radios 277
Disabling or Reenabling Radios 277
Enabling or Disabling Individual Radios 278
Disabling or Reenabling All Radios Using a Profile 279
Resetting a Radio to its Factory Default Settings 280
Restarting an AP 281
Displaying AP Information 281
Displaying AP Configuration Information 282
Displaying a List of Distributed APs 283
Displaying a List of Distributed APs that Are Not Configured 284
Displaying Connection Information for Distributed APs 285
Displaying Service Profile Information 286
Displaying Radio Profile Information 287
Displaying AP Status Information 288
Displaying AP Statistics Counters 289

Configuring RF Auto-Tuning 291

RF Auto-Tuning Overview 291
Initial Channel and Power Assignment 292

Channel and Power Tuning 293
RF Auto-Tuning Parameters 295
Changing RF Auto-Tuning Settings 296
Changing Channel Tuning Settings 297
Changing Power Tuning Settings 298
Changing the Minimum Transmit Data Rate 300
Displaying RF Auto-Tuning Information 300
Displaying RF Auto-Tuning Settings 301
Displaying RF Neighbors 302
Displaying RF Attributes 303

Wi-Fi Multimedia 305

How WMM Works in WSS Software 305
QoS on the WSS Switch 306
QoS on an AP 307
Disabling or Reenabling WMM 308
Displaying WMM Information 309

Configuring and Managing Spanning Tree Protocol 311

Enabling the Spanning Tree Protocol 312
Changing Standard Spanning Tree Parameters 313
Changing the Bridge Priority 315
Changing STP Port Parameters 316
Changing Spanning Tree Timers 318
Configuring and Managing STP Fast Convergence Features 319
Configuring Port Fast Convergence 321
Displaying Port Fast Convergence Information 322
Configuring Backbone Fast Convergence 323
Displaying the Backbone Fast Convergence State 324
Configuring Uplink Fast Convergence 325
Displaying Uplink Fast Convergence Information 326
Displaying Spanning Tree Information 326
Displaying STP Bridge and Port Information 327
Displaying the STP Port Cost on a VLAN Basis 328
Displaying Blocked STP Ports 329
Displaying Spanning Tree Statistics 330

Clearing STP Statistics 332
Spanning Tree Configuration Scenario 332

Configuring and Managing IGMP Snooping 335

Disabling or Reenabling IGMP Snooping 335
Disabling or Reenabling Proxy Reporting 335
Enabling the Pseudo-Querier 336
Changing IGMP Timers 336
Changing the Query Interval 337
Changing the Other-Querier-Present Interval 338
Changing the Query Response Interval 339
Changing the Last Member Query Interval 340
Changing Robustness 341
Enabling Router Solicitation 341
Changing the Router Solicitation Interval 342
Configuring Static Multicast Ports 342
Adding or Removing a Static Multicast Router Port 343
Adding or Removing a Static Multicast Receiver Port 344
Displaying Multicast Information 344
Displaying Multicast Configuration Information and Statistics 345
Displaying Multicast Queriers 347
Displaying Multicast Routers 348
Displaying Multicast Receivers 349

Configuring and Managing Security ACLs 351

About Security Access Control Lists 351
Overview of Security ACL Commands 352
Security ACL Filters 353
Creating and Committing a Security ACL 353
Setting a Source IP ACL 354
Setting an ICMP ACL 357
Setting TCP and UDP ACLs 359
Determining the ACE Order 361
Committing a Security ACL 362
Viewing Security ACL Information 363
Clearing Security ACLs 365

Mapping Security ACLs 365
Mapping User-Based Security ACLs 366
Mapping Security ACLs to Ports, VLANs, Virtual Ports, or Distributed APs . 368
Modifying a Security ACL 369
Adding Another ACE to a Security ACL 370
Placing One ACE before Another 371
Modifying an Existing Security ACL 372
Clearing Security ACLs from the Edit Buffer 373
Using ACLs to Change CoS 374
Filtering Based on DSCP Values 375
Enabling Prioritization for Legacy Voice over IP 376
Enabling SVP Optimization for SpectraLink Phones 377
Security ACL Configuration Scenario 377

Managing Keys and Certificates 379

Why Use Keys and Certificates? 379
Wireless Security through TLS 380
PEAP-MS-CHAP-V2 Security 381
About Keys and Certificates 381
Public Key Infrastructures 382
Public and Private Keys 383
Digital Certificates 384
PKCS #7, PKCS #10, and PKCS #12 Object Files 385
Creating Keys and Certificates 385
Choosing the Appropriate Certificate Installation Method for Your Network . 387
Creating Public-Private Key Pairs 388
Generating Self-Signed Certificates 389
Installing a Key Pair and Certificate from a PKCS #12 Object File 390
Creating a CSR and Installing a Certificate from a PKCS #7 Object File . . . 391
Installing a CA's Own Certificate 392
Displaying Certificate and Key Information 393
Key and Certificate Configuration Scenarios 393
Creating Self-Signed Certificates 394
Installing CA-Signed Certificates from PKCS #12 Object Files 397
Installing CA-Signed Certificates Using a PKCS #10 Object File (CSR) and a PKCS #7 Object File 399

Configuring AAA for Network Users 401
About AAA for Network Users 401
Authentication 402
Authorization 408
Accounting 409
Summary of AAA Features 410
AAA Tools for Network Users 410
“Wildcards” and Groups for Network User Classification 411
AAA Methods for IEEE 802.1X and Web Network Access 412
IEEE 802.1X Extensible Authentication Protocol Types 415
Ways an WSS Switch Can Use EAP 416
Effects of Authentication Type on Encryption Method 417
Configuring 802.1X Authentication 417
Configuring 802.1X Acceleration 418
Using Pass-Through 419
Authenticating through a Local Database 420
Binding User Authentication to Machine Authentication 421
Configuring Authentication and Authorization by MAC Address 425
Adding and Clearing MAC Users and User Groups Locally 426
Configuring MAC Authentication and Authorization 427
Changing the MAC Authorization Password for RADIUS 428
Configuring Web-based AAA 428
How Portal Web-based AAA Works 429
Web-based AAA Requirements and Recommendations 430
Configuring Portal Web-based AAA 433
Using a Custom Login Page 436
Using Dynamic Fields in Web-based AAA Redirect URLs 439
Configuring Last-Resort Access 440
Configuring AAA for Users of Third-Party APs 441
Authentication Process for 802.1X Users of a Third-Party AP 442
Requirements 443
Configuring Authentication for 802.1X Users of a Third-Party AP 444
Assigning Authorization Attributes 446
Assigning Attributes to Users and Groups 450
Assigning a Security ACL to a User or a Group 451

Clearing a Security ACL from a User or Group 453
Assigning Encryption Types to Wireless Users 454
Overriding or Adding Attributes Locally with a Location Policy 455
About the Location Policy 456
How the Location Policy Differs from a Security ACL 457
Setting the Location Policy 458
Clearing Location Policy Rules and Disabling the Location Policy 460
Configuring Accounting for Wireless Network Users 460
Viewing Local Accounting Records 462
Viewing Roaming Accounting Records 463
Displaying the AAA Configuration 464
Avoiding AAA Problems in Configuration Order 465
Using the Wildcard “Any” as the SSID Name in Authentication Rules 465
Using Authentication and Accounting Rules Together 467
Configuring a Mobility Profile 468
Network User Configuration Scenarios 469
General Use of Network User Commands 470
Enabling RADIUS Pass-Through Authentication 472
Enabling PEAP-MS-CHAP-V2 Authentication 473
Enabling PEAP-MS-CHAP-V2 Offload 474
Combining 802.1X Acceleration with Pass-Through Authentication 475
Overriding AAA-Assigned VLANs 476

Configuring Communication with RADIUS 477

RADIUS Overview 477
Before You Begin 479
Configuring RADIUS Servers 479
Configuring Global RADIUS Defaults 480
Setting the System IP Address as the Source Address 481
Configuring Individual RADIUS Servers 482
Deleting RADIUS Servers 483
Configuring RADIUS Server Groups 483
Creating Server Groups 484
Deleting a Server Group 487
RADIUS and Server Group Configuration Scenario 487

Managing 802.1X on the WSS Switch 489

Managing 802.1X on Wired Authentication Ports 489
Enabling and Disabling 802.1X Globally 490
Setting 802.1X Port Control 491
Managing 802.1X Encryption Keys 491
Enabling 802.1X Key Transmission 492
Configuring 802.1X Key Transmission Time Intervals 493
Managing WEP Keys 494
Setting EAP Retransmission Attempts 495
Managing 802.1X Client Reauthentication 495
Enabling and Disabling 802.1X Reauthentication 496
Setting the Maximum Number of 802.1X Reauthentication Attempts 497
Setting the 802.1X Reauthentication Period 498
Setting the Bonded Authentication Period 499
Managing Other Timers 499
Setting the 802.1X Quiet Period 500
Setting the 802.1X Timeout for an Authorization Server 501
Setting the 802.1X Timeout for a Client 502
Displaying 802.1X Information 502
Viewing 802.1X Clients 503
Viewing the 802.1X Configuration 504
Viewing 802.1X Statistics 505

Managing Sessions 507

About the Session Manager 507
Displaying and Clearing Administrative Sessions 507
Displaying and Clearing All Administrative Sessions 508
Displaying and Clearing an Administrative Console Session 509
Displaying and Clearing Administrative Telnet Sessions 510
Displaying and Clearing Client Telnet Sessions 511
Displaying and Clearing Network Sessions 511
Displaying Verbose Network Session Information 512
Displaying and Clearing Network Sessions by Username 513
Displaying and Clearing Network Sessions by MAC Address 514
Displaying and Clearing Network Sessions by VLAN Name 515

Displaying and Clearing Network Sessions by Session ID 516

Managing System Files 517

About System Files 517
Displaying Software Version Information 518
Displaying Boot Information 520
Working with Files 520
Displaying a List of Files 521
Copying a File 522
Deleting a File 524
Creating a Subdirectory 525
Removing a Subdirectory 526
Managing Configuration Files 526
Displaying the Running Configuration 527
Saving Configuration Changes 529
Specifying the Configuration File to Use After the Next Reboot 530
Loading a Configuration File 531
Resetting to the Factory Default Configuration 532
Backing Up and Restoring the System 532
Managing Configuration Changes 534
Backup and Restore Examples 535
Upgrading the System Image 535

Rogue Detection and Countermeasures 537

About Rogues and RF Detection 537
Rogue access points and Clients 538
RF Detection Scans 541
Countermeasures 542
Summary of Rogue Detection Features 542
Configuring Rogue Detection Lists 543
Configuring a Permitted Vendor List 544
Configuring a Permitted SSID List 545
Configuring a Client Black List 546
Configuring an Attack List 547
Configuring an Ignore List 548
Enabling Countermeasures 548

Disabling or Reenabling Active Scan 549
Enabling AP Signatures 549
Disabling or Reenabling Logging of Rogues 550
Enabling Rogue and Countermeasures Notifications 550
IDS and DoS Alerts 550
Flood Attacks 551
DoS Attacks 552
Netstumbler and Wellenreiter Applications 553
Wireless Bridge 554
Ad-Hoc Network 555
Weak WEP Key Used by Client 556
Disallowed Devices or SSIDs 557
Displaying Statistics Counters 558
IDS Log Message Examples 559
Displaying RF Detection Information 561
Displaying Rogue Clients 563
Displaying Rogue Detection Counters 564
Displaying SSID or BSSID Information for a Mobility Domain 565
Displaying RF Detect Data 567
Displaying the APs Detected by an AP Radio 568
Displaying Countermeasures Information 569

Troubleshooting a WS Switch 571

Fixing Common WSS Setup Problems 572
Recovering the System Password 574
WSS-2350 574
WSS-2370, WSS-2380, or WSS-2360 574
Configuring and Managing the System Log 575
Log Message Components 575
Logging Destinations and Levels 576
Using Log Commands 578
Running Traces 582
Using the Trace Command 582
Displaying a Trace 583
Stopping a Trace 583
About Trace Results 584

Displaying Trace Results 584
Copying Trace Results to a Server 585
Clearing the Trace Log 585
List of Trace Areas 585
Using Show Commands 586
Viewing VLAN Interfaces 586
Viewing AAA Session Statistics 586
Viewing FDB Information 587
Viewing ARP Information 587
Remotely Monitoring Traffic 588
How Remote Traffic Monitoring Works 588
Best Practices for Remote Traffic Monitoring 588
Configuring a Snoop Filter 590
Mapping a Snoop Filter to a Radio 591
Enabling or Disabling a Snoop Filter 592
Displaying Remote Traffic Monitoring Statistics 594
Preparing an Observer and Capturing Traffic 594
Capturing System Information for Technical Support 595
Displaying Technical Support Information 596
Sending Information to NETS 597

Supported RADIUS Attributes 599
Supported Standard and Extended Attributes 599
Nortel Vendor-Specific Attributes 603

Mobility Domain Traffic Ports 605

DHCP Server 607
How the WSS Software DHCP Server Works 608
Configuring the DHCP Server 608
Displaying DHCP Server Information 609

Glossary 611

Index 633

Command Index 653

How to get Help

This section explains how to get help for Nortel products and services.

Getting Help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

http://www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting Help over the phone from a Nortel Solutions Center

If you don't find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

http://www.nortel.com/callus

Getting Help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Introducing the Nortel WLAN 2300 System

Nortel WLAN 2300 System 31
Documentation 32

This guide explains how to configure and manage a Nortel WLAN 2300 System wireless LAN (WLAN) using the WLAN 2300 System Software command line interface (CLI) commands that you enter on a WLAN—Security Switch (WSS).

Read this guide if you are a network administrator or other person configuring and managing one or more switches and Access Points (AP) in a network.

Nortel WLAN 2300 System

The Nortel WLAN 2300 System is an enterprise-class WLAN solution that seamlessly integrates with an existing wired enterprise network. The Nortel system provides secure connectivity to both wireless and wired users in large environments such as office buildings, hospitals, and university campuses and in small environments such as branch offices.

The Nortel WLAN 2300 System fulfills the three fundamental requirements of an enterprise WLAN: It eliminates the distinction between wired and wireless networks, allows users to work safely from anywhere (*secure mobility*), and provides a comprehensive suite of intuitive tools for planning and managing the network before and after deployment, greatly easing the operational burden on IT resources.

The Nortel WLAN 2300 System consists of the following components:

- **WLAN Management Software tool suite**—A full-featured graphical user interface (GUI) client application used to plan, configure, and deploy a WLAN and its users. It also provides a centralized service application for WLAN and user monitoring, reporting, and diagnostics
- **One or more WLAN—Security Switch (WSS)** —Distributed, intelligent machines for managing user connectivity, connecting and powering Access Points (AP) access ports, and connecting the WLAN to the wired network backbone
- **Multiple Access Points (AP)** —Wireless access points (AP) that transmit and receive radio frequency (RF) signals to and from wireless users and connect them to a WSS
- **WLAN 2300 System Software (WSS Software)**—The operating system that runs all WSSs and AP access ports in a WLAN, and is accessible through a command-line interface (CLI), the Web View interface, or the WLAN Management Software GUI

Documentation

Consult the following documents to plan, install, configure, and manage a Nortel WLAN 2300 System.

Planning, Configuration, and Deployment

Nortel WLAN Management Software User's Guide. Instructions for planning, configuring, deploying, and managing the entire WLAN with the WLAN Management Software tool suite. Read this guide to learn how to plan wireless services, how to configure and deploy Nortel equipment to provide those services, and how to optimize and manage your WLAN.

Nortel WLAN Management Software Reference Manual. Detailed instructions and information for all WLAN Management Software planning, configuration, and management features.

Installation

- *Nortel WLAN 2300 System Software Quick Start Guide.* Instructions for performing basic setup of secure (802.1X) and guest (Web-based AAA™) access, for configuring a Mobility Domain for roaming, and for accessing a sample network plan in WLAN Management Software for advanced configuration and management
- *Nortel WLAN—Security Switch Installation and Basic Configuration Guide.* Instructions and specifications for installing an WSS switch in a Nortel WLAN 2300 System WLAN, and basic instructions for deploying a secure IEEE 802.11 wireless service
- *Nortel Access Port Installation Guide*. Instructions and specifications for installing an AP access point and connecting it to a WSS
- *Nortel Regulatory Information*. important safety instructions and compliance information that you must read before installing Nortel products



Note. *Nortel Regulatory Information* is updated frequently. See http://www.nortel.com for the most current version.

Configuration and Management

- *Nortel WLAN Management Software Reference Manual*. Instructions for planning, configuring, deploying, and managing the entire WLAN with the WLAN Management Software tool suite
- *Nortel Mobility System Software Configuration Guide*. Instructions for configuring and managing the system through the WSS Software CLI
- *Nortel Mobility System Software Command Reference.* Functional and alphabetic reference to all WSS Software commands supported on WSSs and AP access points

Safety and Advisory Notices

The following kinds of safety and advisory notices appear in this manual.



Caution! This situation or condition can lead to data loss or damage to the product or other property.



Note. This information is of special interest.

Text and Syntax Conventions

Nortel manuals use the following text and syntax conventions:

Convention	Use
Monospace text	Sets off command syntax or sample commands and system responses.
Bold text	Highlights commands that you enter or items you select.
Italic text	Designates command variables that you replace with appropriate values, or highlights publication titles or words requiring special emphasis.
Menu Name > Command	Indicates a menu item that you select. For example, **File > New** indicates that you select **New** from the File menu.
[ ] (square brackets)	Enclose optional parameters in command syntax.
{ } (curly brackets)	Enclose mandatory parameters in command syntax.
| (vertical bar)	Separates mutually exclusive options in command syntax.

Using the Command-Line Interface

CLI Conventions 35
Command-Line Editing 43
Using CLI Help 49
Understanding Command Descriptions 50

WLAN 2300 System Software (WSS Software) operates a Nortel WLAN 2300 System wireless LAN (WLAN) consisting of WLAN Management Software software, WLAN—Security Switch (WSS) switches, and Access Point (AP) access points. WSS Software has a command-line interface (CLI) on the WSS switch that you can use to configure and manage the switch and its attached AP access points.

You configure the WSS and AP access points primarily with **set**, **clear**, and **show** commands. Use **set** commands to change parameters. Use **clear** commands to reset parameters to their defaults. In many cases, you can overwrite a parameter with another **set** command. Use **show** commands to display the current configuration and monitor the status of network operations.

The WSS supports two connection modes:

- Administrative access mode, which enables the network administrator to connect *to* the WSS and configure the network
- Network access mode, which enables network users to connect *through* the WSS to access the network

CLI Conventions

Be aware of the following WSS Software CLI conventions for command entry:

- "Command Prompts" on page 36
- "Syntax Notation" on page 37
- "Text Entry Conventions and Allowed Characters" on page 38
- "User Wildcards, MAC Address Wildcards, and VLAN Wildcards" on page 39
- "Port Lists" on page 41
- "Virtual LAN Identification" on page 42

Command Prompts

By default, the WSS Software CLI provides the following prompt for restricted users. The *mm* portion shows the WSS switch model number (for example, *2370*) and the *nnnnnn* portion shows the last 6 digits of the switch's media access control (MAC) address.

```
NT-mm-nnnnnn>
```

After you become enabled as an administrative user by typing **enable** and supplying a suitable password, WSS Software displays the following prompt:

```
NT-mm-nnnnnn#
```

For ease of presentation, this manual shows the restricted and enabled prompts as follows:

```
23xx>
```

```
23xx#
```

For information about changing the CLI prompt on a WSS, see the **set prompt** command description in the *Nortel WLAN 2300 Series System Software Command Reference.*

Syntax Notation

The WSS Software CLI uses standard syntax notation:

- Bold monospace font identifies the command and keywords you must type. For example:

  set enablepass

- Italic monospace font indicates a placeholder for a value. For example, you replace *vlan-id* in the following command with a virtual LAN (VLAN) ID:

  clear interface *vlan-id* **ip**

- Curly brackets ({ }) indicate a mandatory parameter, and square brackets ([ ]) indicate an optional parameter. For example, you must enter **dynamic** or **port** and a port list in the following command, but a VLAN ID is optional:

  clear fdb {**dynamic** | **port** *port-list*} [**vlan** *vlan-id*]

- A vertical bar (|) separates mutually exclusive options within a list of possibilities. For example, you enter either **enable** or **disable**, not both, in the following command:

  set port {**enable** | **disable**} *port-list*

Text Entry Conventions and Allowed Characters

Unless otherwise indicated, the WSS Software CLI accepts standard ASCII alphanumeric characters, except for tabs and spaces, and is case-insensitive.

The CLI has specific notation requirements for MAC addresses, IP addresses, and masks, and allows you to group usernames, MAC addresses, virtual LAN (VLAN) names, and ports in a single command.

Nortel recommends that you do not use the same name with different capitalizations for VLANs or access control lists (ACL). For example, do not configure two separate VLANs with the names *red* and *RED*.

The CLI does not support the use of special characters including the following in any named elements such as SSIDs and VLANs: ampersand (&), angle brackets (< >), number sign (#), question mark (?), or quotation marks (“”).

In addition, the CLI does not support the use of international characters such as the accented *É* in DÉCOR.

MAC Address Notation

WSS Software displays MAC addresses in hexadecimal numbers with a colon (:) delimiter between bytes—for example, 00:01:02:1a:00:01. You can enter MAC addresses with either hyphen (-) or colon (:) delimiters, but colons are preferred.

For shortcuts:

- You can exclude leading zeros when typing a MAC address. WSS Software displays of MAC addresses include all leading zeros.
- In some specified commands, you can use the single-asterisk (*) wildcard character to represent an entire MAC address or from 1 byte to 5 bytes of the address. (For more information, see “MAC Address Wildcards” on page 39.)

IP Address and Mask Notation

WSS Software displays IP addresses in dotted decimal notation—for example, 192.168.1.111. WSS Software makes use of both subnet masks and wildcard masks.

Subnet Masks

Unless otherwise noted, use classless interdomain routing (CIDR) format to express subnet masks—for example, 192.168.1.112/24. You indicate the subnet mask with a forward slash (/) and specify the number of bits in the mask.

Wildcard Masks

Security access control lists (ACL) use source and destination IP addresses and wildcard masks to determine whether the WSS filters or forwards IP packets. Matching packets are either permitted or denied network access. The ACL checks the bits in IP addresses that correspond to any *0*s (zeros) in the mask, but does not check the bits that correspond to *1*s (ones) in the mask. You specify the wildcard mask in dotted decimal notation.

For example, the address 10.0.0.0 and mask 0.255.255.255 match all IP addresses that begin with 10 in the first octet.

User Wildcards, MAC Address Wildcards, and VLAN Wildcards

Name "globbing" is a way of using a wildcard pattern to expand a single element into a list of elements that match the pattern. WSS Software accepts user globs, MAC address globs, and VLAN globs. The order in which globs appear in the configuration is important, because once a wildcard is matched, processing stops on the list of globs

User Wildcards

A user wildcard is shorthand method for matching an authentication, authorization, and accounting (AAA) command to either a single user or a set of users.

A user wildcard can be up to 80 characters long and cannot contain spaces or tabs. The double-asterisk (**) wildcard characters with no delimiter characters match *all* usernames. The single-asterisk (*) wildcard character matches any number of characters up to, but not including, a delimiter character in the wildcard. Valid user wildcard delimiter characters are the *at* (@) sign and the period (.).

For example, the following globs identify the following users:

User Wildcard	User Designated
jose@example.com	User *jose* at example.com
*@example.com	All users at example.com whose usernames do not contain periods—for example, jose@example.com and tamara@example.com, but *not* nin.wong@example.com, because nin.wong contains a period
*@marketing.example.com	All marketing users at example.com whose usernames do not contain periods
.@marketing.example.com	All marketing users at example.com whose usernames contain a period
*	All users with usernames that have no delimiters
EXAMPLE*	All users in the Windows Domain EXAMPLE with usernames that have no delimiters
EXAMPLE*.*	All users in the Windows Domain EXAMPLE whose usernames contain a period
**	All users

MAC Address Wildcards

A media access control (MAC) address wildcard is a similar method for matching some authentication, authorization, and accounting (AAA) and forwarding database (FDB) commands to one or more 6-byte MAC addresses. In a MAC address wildcard, you can use a single asterisk (*) as a wildcard to match *all* MAC addresses, or as follows to match from 1 byte to 5 bytes of the MAC address:

```
00:*
00:01:*
```

```
00:01:02:*
00:01:02:03:*
00:01:02:03:04:*
```

For example, the MAC address wildcard 02:06:8c* represents all MAC addresses starting with 02:06:8c. Specifying only the first 3 bytes of a MAC address allows you to apply commands to MAC addresses based on an organizationally unique identity (OUI).

VLAN Wildcards

A VLAN wildcard is a method for matching one of a set of local rules on an WSS switch, known as the location policy, to one or more users. WSS Software compares the VLAN wildcard, which can optionally contain wildcard characters, against the VLAN-Name attribute returned by AAA, to determine whether to apply the rule.

To match *all* VLANs, use the double-asterisk (**) wildcard characters with no delimiters. To match any number of characters up to, but not including, a delimiter character in the wildcard, use the single-asterisk (*) wildcard. Valid VLAN wildcard delimiter characters are the *at* (@) sign and the period (.).

For example, the VLAN wildcard *bldg4.** matches *bldg4.security* and *bldg4.hr* and all other VLAN names with *bldg4.* at the beginning.

Matching Order for Wildcards

In general, the order in which you enter AAA commands determines the order in which WSS Software matches the user, MAC address, or VLAN to a wildcard. To verify the order, view the output of the **show aaa** or **show config** command. WSS Software checks globs that appear higher in the list before items lower in the list and uses the first successful match.

Port Lists

The physical Ethernet ports on a WSS can be set for connection to AP access points, authenticated wired users, or the network backbone. You can include a single port or multiple ports in one WSS Software CLI command by using the appropriate list format.

The ports on a WSS are numbered 1 through 22. No port 0 exists on the switch. You can include a single port or multiple ports in a command that includes **port** *port-list*. Use one of the following formats for *port-list*:

- A single port number. For example:

```
23x0# set port enable 16
```

- A comma-separated list of port numbers, with no spaces. For example:

```
23x0# show port poe 1,2,4,13
```

- A hyphen-separated range of port numbers, with no spaces. For example:

```
23x0# reset port 12-16
```

- Any combination of single numbers, lists, and ranges. Hyphens take precedence over commas. For example:

```
23x0# show port status 1-3,14
```

Virtual LAN Identification

The *names* of virtual LANs (VLAN), which are used in Mobility Domain™ communications, are set by you and can be changed. In contrast, VLAN ID *numbers*, which the WSS uses locally, are determined when the VLAN is first configured and cannot be changed. Unless otherwise indicated, you can refer to a VLAN by either its VLAN name or its VLAN number. CLI **set** and **show** commands use a VLAN's name or number to uniquely identify the VLAN within the WSS.

Command-Line Editing

WSS Software editing functions are similar to those of many other network operating systems.

Keyboard Shortcuts

The following keyboard shortcuts are available for entering and editing CLI commands:

Keyboard Shortcuts	Function
Ctrl+A	Jumps to the first character of the command line.
Ctrl+B or Left Arrow key	Moves the cursor back one character.
Ctrl+C	Escapes and terminates prompts and tasks.
Ctrl+D	Deletes the character at the cursor.
Ctrl+E	Jumps to the end of the current command line.
Ctrl+F or Right Arrow key	Moves the cursor forward one character.
Ctrl+K	Deletes from the cursor to the end of the command line.
Ctrl+L or Ctrl+R	Repeats the current command line on a new line.
Ctrl+N or Down Arrow key	Enters the next command line in the history buffer.
Ctrl+P or Up Arrow key	Enters the previous command line in the history buffer.
Ctrl+U or Ctrl+X	Deletes characters from the cursor to the beginning of the command line.
Ctrl+W	Deletes the last word typed.
Esc B	Moves the cursor back one word.
Esc D	Deletes characters from the cursor forward to the end of the word.
Delete key or Backspace key	Erases mistake made during command entry. Reenter the command after using this key.

History Buffer

The history buffer stores the last 63 commands you entered during a terminal session. You can use the Up Arrow and Down Arrow keys to select a command that you want to repeat from the history buffer.

Tabs

The WSS Software CLI uses the Tab key for command completion. You can type the first few characters of a command and press the Tab key to display the commands that begin with those characters. For example:

```
23x0# show i <Tab>
ifm         Show interfaces maintained by the interface manager
igmp        Show igmp information
interface   Show interfaces
ip          Show ip information
```

Single-Asterisk (*) Wildcard Character

You can use the single-asterisk (*) wildcard character in globbing. (For details, see "User Wildcards, MAC Address Wildcards, and VLAN Wildcards" on page 39.)

Double-Asterisk (**) Wildcard Characters

The double-asterisk (**) wildcard character matches all usernames. For details, see “User Wildcards” on page 39.

Using CLI Help

The CLI provides online help. To see the full range of commands available at your access level, type the following command:

```
23x0# help
Commands:
--------------------------------------------------------------------------
clear                  Clear, use 'clear help' for more information
commit                 Commit the content of the ACL table
copy                   Copy from filename (or url) to filename (or url)
crypto                 Crypto, use 'crypto help' for more information
delete                 Delete url
dir                    Show list of files on flash device
disable                Disable privileged mode
exit                   Exit from the Admin session
help                   Show this help screen
history                Show contents of history substitution buffer
hit-sample-rate        Set NP hit-counter sample rate
load                   Load, use 'load help' for more information
logout                 Exit from the Admin session
monitor                Monitor, use 'monitor help' for more information
ping                   Send echo packets to hosts
quit                   Exit from the Admin session
reset                  Reset, use 'reset help' for more information
rollback               Remove changes to the edited ACL table
save                   Save the running configuration to persistent storage
set                    Set, use 'set help' for more information
show                   Show, use 'show help' for more information
telnet                 telnet IP address [server port]
traceroute             Print the route packets take to network host
```

For more information on help, see the **help** command description in the *Nortel WLAN Security Switch 2300 Software Command Reference*.

To see a subset of the online help, type the command for which you want more information. For example, the following command displays all the commands that begin with the letter *i*:

```
23x0# show i?
ifm                    Showinterfacesmaintainedbytheinterfacemanager
igmp                    Show igmp information
interface               Show interfaces
ip                      Show ip information
```

To see all the variations, type one of the commands followed by a question mark (?). For example:

```
23x0# show ip ?
alias                   Show ip aliases
dns                     show DNS status
https                   show ip https
route                   Show ip route table
telnet                  show ip telnet
```

To determine the port on which Telnet is running, type the following command:

```
23x0# show ip telnet
Server Status                  Port
---------------------------------
Enabled                         23
```

Understanding Command Descriptions

Each command description in the *Nortel WLAN Security Switch 2300 Software Command Reference* contains the following elements:

- A command name, which shows the keywords but not the variables. For example, the following command name appears at the top of a command description and in the index:

  ```
  set {ap | dap} name
  ```

  The **set {ap | dap} name** command has the following complete syntax:

  set {**ap** *port-list* | **dap** *dap-num*} **name** *name*

- A brief description of the command's functions.
- The full command syntax.
- Any command defaults.
- The command access, which is either *enabled* or *all*. *All* indicates that anyone can access this command. *Enabled* indicates that you must enter the enable password before entering the command.
- The command history, which identifies the WSS Software version in which the command was introduced and the version numbers of any subsequent updates.
- Special tips for command usage. These are omitted if the command requires no special usage.
- One or more examples of the command in context, with the appropriate system prompt and response.
- One or more related commands.

Configuring AAA for Administrative and Local Access

Overview of AAA for Administrative and Local Access 51
Before You Start 53
About Administrative Access 54
First-Time Configuration using the Console 56
Configuring Accounting for Administrative Users 63
Displaying the AAA Configuration 65
Saving the Configuration 65
Administrative AAA Configuration Scenarios 66

Overview of AAA for Administrative and Local Access

Nortel WLAN 2300 System Software (WSS Software) supports authentication, authorization, and accounting (AAA) for secure network connections. As administrator, you must establish administrative access for yourself and optionally other local users before you can configure the WSS for operation.

Here is an overview of configuration topics:

1 **Console connection**. By default, any administrator can connect to the console port and manage the switch, because no authentication is enforced. (Nortel recommends that you enforce authentication on the console port after initial connection.)

2 **Telnet or SSH connection**. Administrators cannot establish a Telnet or Secure Shell (SSH) connection to the WSS by default. To provide Telnet or SSH access, you must add a username and password entry to the local database or, optionally, set the authentication method for Telnet users to a Remote Authentication Dial-In User Service (RADIUS) server.



Note. A CLI Telnet connection to the WSS is not secure, unlike SSH, WLAN Management Software and Web View connections. (For details, see Chapter , “Managing Keys and Certificates,” on page 379.)

3 **Restricted mode.** When you initially connect to the WSS, your mode of operation is restricted. In this mode, only a small subset of status and monitoring commands is available. Restricted mode is useful for

administrators with basic monitoring privileges who are not allowed to change the configuration or run traces.

4 **Enabled mode.** To enter the enabled mode of operation, you type the **enable** command at the command prompt. In enabled mode, you can use all CLI commands. Although WSS Software does not require an enable password, Nortel highly recommends that you set one.

5 **Customized authentication.** You can require authentication for all users or for only a subset of users. Username globbing (see "User Wildcards, MAC Address Wildcards, and VLAN Wildcards" on page 39) allows different users or classes of user to be given different authentication treatments. You can configure console authentication and Telnet authentication separately, and you can apply different authentication methods to each.

   For any user, authorization uses the same methods as authentication for that user.

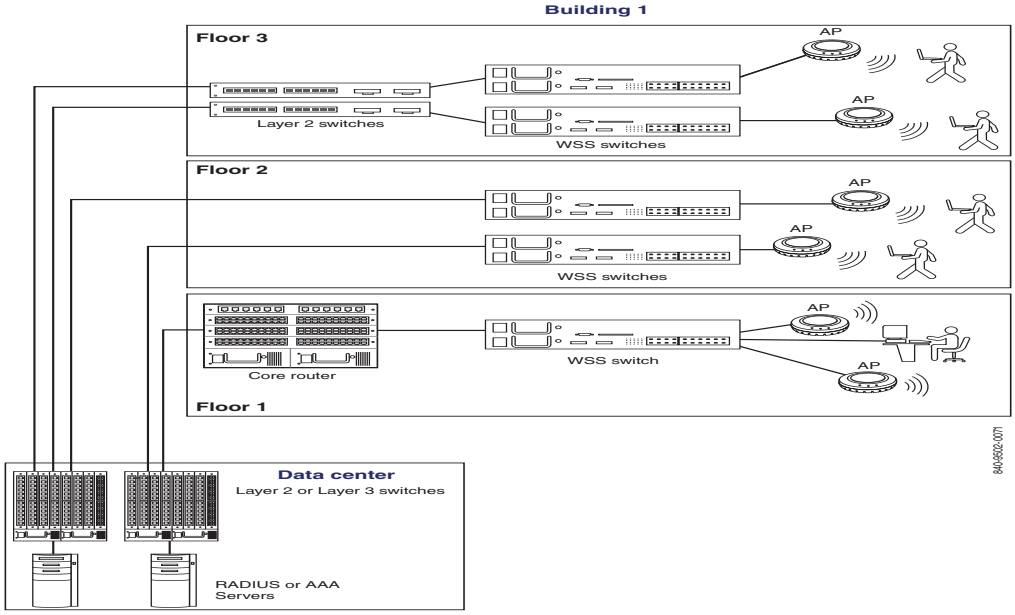
6 **Local override.** A special authentication technique called local override lets you attempt authentication through the local database before attempting authentication through a RADIUS server. The WSS attempts administrative authentication in the local database first. If it finds no match, the WSS attempts administrative authentication on the RADIUS server. (For information about setting a WSS to use RADIUS servers, see Chapter , "Configuring Communication with RADIUS," on page 477.)

7 **Accounting for administrative access sessions.** Accounting records can be stored and displayed locally or sent to a RADIUS server. Accounting records provide an audit trail of the time an administrative user logged in, the administrator's username, the number of bytes transferred, and the time the session started and ended.

Figure 1 on page 53 illustrates a typical WSS, AP access points, and network administrator in an enterprise network. As network administrator, you initially access the WSS through the console. You can then optionally configure authentication, authorization, and accounting for administrative access mode.

Nortel recommends enforcing authentication for administrative access using usernames and passwords stored either locally or on RADIUS servers.

Figure 1: Typical Nortel WLAN 2300 System



Before You Start

Before reading more of this chapter, read the *Nortel WLAN—Security Switch 2300 Series Installation and Basic Configuration Guide* for information about setting up a WSS switch and the attached AP access points for basic service. The following tasks are covered in Chapter 4 of that guide.

1. Accessing the CLI
2. Configuring an enable password
3. Configuring the time and date
4. Installing the software license
5. Configuring IP connectivity
6. Enabling secure communication for WLAN Management Software or Web View
7. Specifying the country of operation
8. Specifying a system IP address
9. Configuring ports for authenticating users
10. Configuring Mobility Domain parameters
11. Configuring user authentication

12 Displaying and saving the configuration

Except for software license installation, these tasks are covered in greater depth in this manual so that you can reconfigure your network as needed.

About Administrative Access

The authentication, authorization, and accounting (AAA) framework helps secure network connections by identifying who the user is, what the user can access, and the amount of network resources the user can consume.

Access Modes

WSS Software provides AAA either locally or through remote servers to authenticate valid users. WSS Software provides two modes of access:

- Administrative access mode—Allows a network administrator to access the WSS and configure it.

  You must establish administrative access in enabled mode before adding users. See "Enabling an Administrator" on page 57.

- Network access mode—Allows network users to connect through the WSS. For information about configuring network users, see Chapter , "Configuring AAA for Network Users," on page 401.

Types of Administrative Access

WSS Software allows you access to the WSS with the following types of administrative access:

- Console—Access through only the console port. For more information, see "First-Time Configuration using the Console" on page 56.
- Telnet—Users who access WSS Software through the Telnet protocol. For information about setting up a WSS for Telnet access, see Chapter , "Configuring and Managing IP Interfaces and Services," on page 107.
- Secure Shell (SSH)—Users who access WSS Software through the SSH protocol. For information about setting up an WSS switch for SSH access, see Chapter , "Configuring and Managing IP Interfaces and Services," on page 107.
- WLAN Management Software —After you configure the WSS as described in the *Nortel WLAN—Security Switch Installation and Basic Configuration Guide*, you can further configure the WSS using the WMS tool suite. For more information, see the *Nortel WLAN Management Software Reference Manual.*
- Web View—A Web-based application for configuring and managing a single WSS through a Web browser. Web View uses a secure connection through Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS).

First-Time Configuration using the Console

Administrators must initially configure the WSS with a computer or terminal connected to the WSS console port through a serial cable. Telnet access is not initially enabled.

To configure a previously unconfigured WSS through the console, you must complete the following tasks:

- Enable an administrator. (See "Enabling an Administrator" on page 57.)
- Configure authentication. (See "Authenticating at the Console" on page 60.)
- Optionally, configure accounting. (see "Configuring Accounting for Administrative Users" on page 63.)
- Save the configuration. (See "Saving the Configuration" on page 65.)

Enabling an Administrator

To enable yourself as an administrator, you must log in to the WSS from the console. Until you set the enable password and configure authentication, the default username and password are blank. Press Enter when prompted for them.

To enable an administrator:

1. Log in to the WSS from the serial console, and press Enter when the WSS displays a username prompt:

   ```
   Username:
   ```

2. Press Enter when the WSS displays a password promptprompt.

   ```
   Password:
   ```

3. Type **enable** to go into enabled mode.

   ```
   23x0> enable
   ```

4. Press Enter to display an enabled-mode command prompt:

   ```
   23x0#
   ```

   Once you see this prompt after you have typed the **enable** command, you have administrative privileges, which allow you to further configure the WSS.

Setting the WSS Switch Enable Password

There is one enable password for the entire WSS. You can optionally change the enable password from the default.

Caution! Nortel recommends that you change the enable password from the default (no password) to prevent unauthorized users from entering configuration commands.

Setting the WSS Enable Password for the First Time

To set the enable password for the first time:

1. At the enabled prompt, type **set enablepass.**
2. At the "Enter old password" prompt, press Enter.
3. At the "Enter new password" prompt, enter an enable password of up to 32 alphanumeric characters with no spaces. The password is not displayed as you type it.

Note. The enable password is case-sensitive.

4. Type the password again to confirm it.

   WSS Software lets you know the password is set.

```
23x0# set enablepass

Enter old password:
Enter new password:
Retype new password:
Password changed
```

Caution! Be sure to use a password that you will remember. If you lose the enable password, the only way to restore it causes the system to return to its default settings and wipes out any saved configuration. (For details, see "Recovering the System Password" on page 574.)

5. Store the configuration into nonvolatile memory by typing the following command:

```
23x0# save config
success: configuration saved.
```

WMS Enable Password

If you are using WMS, you must use the same enable password on WMS that you use on the WSS. After you install the administrative certificate on the WSS and configure basic connectivity, you can configure the rest of your Nortel network AAA settings in WMS.

For connectivity information, see the *Nortel WLAN—Security Switch Installation and Basic Configuration Guide*. For WMS information, see the *Nortel WLAN Management Software Reference Manual*.

Authenticating at the Console

You can configure the console so that authentication is required, or so that *no* authentication is required. Nortel recommends that you enforce authentication on the console port.

To enforce console authentication, take the following steps:

1. Add a user in the local database by typing the following command with a username and password:

   ```
   23x0# set user username password password
   success: change accepted.
   ```

2. To enforce the use of console authentication through the local database, type the following command:

   Caution! If you type this command before you have created a local username and password, you can lock yourself out of the WSS. Before entering this command, you *must* configure a local username and password.

   ```
   23x0# set authentication console * local
   ```

3. To store this configuration into nonvolatile memory, type the following command:

   ```
   23x0# save config
   success: configuration saved.
   ```

By default, no authentication is required at the console. If you have previously required authentication and have decided not to require it (during testing, for example), type the following command to configure the console so that it does *not* require username and password authentication:

```
23x0# set authentication console * none
```



Note. The authentication method **none** you can specify for administrative access is different from the fallthru authentication type None, which applies only to network access. The authentication method **none** allows access to the WSS switch by an administrator. The fallthru authentication type None denies access to a network user. (For information about the fallthru authentication types, see "Authentication Algorithm" on page 4039.)

Customizing AAA with “Wildcards” and Groups

“Wildcards” lets you classify users by username or media access control (MAC) address for different AAA treatments. A user wildcard is a string, possibly containing wildcards, for matching AAA and IEEE 802.1X authentication methods to a user or set of users. The WSS switch supports the following wildcard characters for user globs:

- Single asterisk (*) matches the characters in a username up to but not including a separator character, which can be an *at* (@) sign or a period (.).
- Double asterisk (**) matches all usernames.

In a similar fashion, MAC address globs match authentication methods to a MAC address or set of MAC addresses. For details, see “User Wildcards, MAC Address Wildcards, and VLAN Wildcards” on page 39.

A user group is a named collection of users or MAC addresses sharing a common authorization policy. For example, you might group all users on the first floor of building 17 into the group *bldg-17-1st-floor*, or group all users in the IT group into the group *infotech-people*. Individual user entries override group entries if they both configure the same attribute.

(For information about configuring users and user groups, see “Adding and Clearing Local Users for Administrative Access” on page 63.)

Setting User Passwords

Like usernames, passwords are case-sensitive. To make passwords secure, make sure they contain uppercase and lowercase letters and numbers. Nortel recommends that all users create passwords that are memorable to themselves, difficult for others to guess, and not subject to a dictionary attack.

User passwords are automatically encrypted when entered in the local database. However, the encryption is not strong. It is designed only to discourage someone looking over your shoulder from memorizing your password as you display the configuration. To maintain security, WSS Software displays only the encrypted form of the password in **show** commands.



Note. Although WSS Software allows you to configure a user password for the special "last-resort" guest user, the password has no effect. Last-resort users can never access an WSS in administrative mode and never require a password.

Adding and Clearing Local Users for Administrative Access

Usernames and passwords can be stored locally on the WSS switch. Nortel recommends that you enforce console authentication after the initial configuration to prevent anyone with unauthorized access to the console from logging in. The local database on the WSS switch is the simplest way to store user information in a Nortel system.

To configure a user in the local database, type the following command:

set user *username* **password** *password*

For example, to configure user Jose with the password *spRin9* in the local database on the WSS, type the following command:

```
23x0# set user Jose password spRin9
success: User Jose created
```

To clear a user from the local database, type the following command:

clear user *username*

Configuring Accounting for Administrative Users

Accounting allows you to track network resources. Accounting records can be updated for three important events: when the user is first connected, when the user roams from one AP access point to another, and when the user terminates his or her session. The default for accounting is *off*.

To configure accounting for administrative logins, use the following command:

set accounting {admin | **console} {***user-wildcard***} {start-stop** | **stop-only}** *method1* [*method2*] [*method3*] [*method4*]

To configure accounting for administrative logins over the network at *EXAMPLE*, enter the following command:

set accounting admin EXAMPLE* start-stop | **stop-only** *aaa-method*

You can select either **start-stop** or **stop-only** accounting modes. The **stop-only** mode sends only stop records, whereas **start-stop** sends both start and stop records, effectively doubling the number of accounting records. In most cases, **stop-only** is entirely adequate for administrative accounting, because a stop record contains all the information you might need about a session.

In the **set accounting** command, you must include AAA methods that specify whether to use the local database or RADIUS server to receive the accounting records. Specify **local**, which causes the processing to be done on the WSS switch, or specify a RADIUS server group. For information about configuring a RADIUS server group, see "Configuring RADIUS Server Groups" on page 483.

For example, you can set accounting for administrative users using the start-stop mode through the local database:

```
23x0# set accounting admin EXAMPLE\* start-stop local
success: change accepted.
```

The accounting records show the date and time of activity, the user's status and name, and other attributes. The **show accounting statistics** command displays accounting records for administrative users after they have logged in to the WSS switch.

For example, the following accounting records show information about user Geetha's sessions:

```
23x0# show accounting statistics
Sep2611:01:48Acct-Status-Type=STARTAcct-Authentic=0User-Name=Geetha
AAA_TTY_ATTR=2 Event-Timestamp=1064599308
Sept2612:50:21Acct-Status-Type=STOPAcct-Authentic=0User-Name=Geetha
AAA_TTY_ATTR=2 Acct-Session-Time=6513 Event-Timestamp=1064605821
Acct-Output-Octets=332 Acct-Input-Octets=61
Sep2612:50:33Acct-Status-Type=STARTAcct-Authentic=0User-Name=Geetha
AAA_TTY_ATTR=2 Event-Timestamp=1064605833
```

(For information about network user accounting, see "Configuring Accounting for Wireless Network Users" on page 460. For information about the fields in the **show accounting statistics** output, see the *Nortel WLAN Security Switch 2300 Software Command Reference.*)

Displaying the AAA Configuration

To display your AAA configuration, type the following command:

```
23x0# show aaa
Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=0 key=(null) author-pass=(null)

Radius Servers
Server                    Addr           Ports   T/o Tries Dead State
--------------------------------------------------------------------------
r1                     192.168.253.1   1812 1813  5    3    0    UP

Server groups

    sg1: r1

set authentication console * local
set authentication admin * local
set accounting admin Geetha stop-only local
set accounting admin * start-stop local

user Geetha
   Password = 1214253d1d19 (encrypted)
```

(For information about the fields in the output, see the *Nortel WLAN Security Switch 2300 Software Command Reference*.)

Saving the Configuration

You must save the configuration for all commands that you enter and want to use for future sessions. After you enter the administrator's AAA configuration, type the following command to maintain these commands in WSS nonvolatile memory:

```
23x0# save config
success: configuration saved.
```

You can also specify a filename for the configuration—for example, *configday*. To do this, type the following command:

```
23x0# save config configday
Configuration saved to configday.
```

You must type the **save config** command to save all configuration changes since the last time you rebooted the WSS switch or saved the configuration. If the WSS switch is rebooted before you have saved the configuration, all changes are lost.

You can also type the **load config** command, which reloads the WSS switch to the last saved configuration or loads a particular configuration filename. (For more information, see "Managing Configuration Files" on page 526.)

Administrative AAA Configuration Scenarios

The following scenarios illustrate typical configurations for administrative and local authentication. For all scenarios, the administrator is Natasha with the password *m@Jor*. (For RADIUS server configuration details, see Chapter , "Configuring Communication with RADIUS," on page 477.)

- "Local Authentication" on page 67
- "Local Authentication for Console Users and RADIUS Authentication for Telnet Users" on page 68
- "Local Override and Backup Local Authentication" on page 69
- "Authentication When RADIUS Servers Do Not Respond" on page 70

Local Authentication

The first time you access an WSS switch, it requires no authentication. (For more information, see "First-Time Configuration using the Console" on page 56.) In this scenario, after the initial configuration of the WSS switch, Natasha is connected through the console and has enabled access.

To enable local authentication for a console user, you must configure a local username. Natasha types the following commands in this order:

```
23x0# set user natasha password m@Jor
User natasha created

23x0# set authentication console * local
success: change accepted.

23x0# save config
success: configuration saved.
```

Local Authentication for Console Users and RADIUS Authentication for Telnet Users

This scenario illustrates how to enable local authentication for console users and RADIUS authentication for Telnet administrative users. To do so, you configure at least one local username for console authentication and set up a RADIUS server for Telnet administrators. Natasha types the following commands in this order:

```
23x0# set user natasha password m@Jor
User natasha created

23x0# set authentication console * local
success: change accepted.

23x0# set radius server r1 address 192.168.253.1 key sunFLOW#$
success: change accepted.
```

Natasha also adds the RADIUS server (*r1*) to the RADIUS server group *sg1*, and configures Telnet administrative users for authentication through the group. She types the following commands in this order:

```
23x0# set server group sg1 members r1
success: change accepted.

23x0# set authentication admin * sg1
success: change accepted.

23x0# save config
success: configuration saved.
```

Local Override and Backup Local Authentication

This scenario illustrates how to enable local override authentication for console users. Local override means that WSS Software attempts authentication first through the local database. If it finds no match for the user in the local database, WSS Software then tries a RADIUS server—in this case, server *r1* in server group *sg1*. Natasha types the following commands in this order:

```
23x0# set user natasha password m@Jor
User natasha created

23x0# set radius server r1 address 192.168.253.1 key sunFLOW#$
success: change accepted.

23x0# set server group sg1 members r1
success: change accepted.

23x0# set authentication console * local sg1
success: change accepted.

23x0# save config
success: configuration saved.
```

Natasha also enables backup RADIUS authentication for Telnet administrative users. If the RADIUS server does not respond, the user is authenticated by the local database in the WSS switch. Natasha types the following commands:

```
23x0# set authentication admin * sg1 local
success: change accepted.

23x0# save config
success: configuration saved.
```

The order in which Natasha enters authentication methods in the **set authentication** command determines the method WSS Software attempts first. The local database is the first method attempted for console users and the last method attempted for Telnet administrators.

Authentication When RADIUS Servers Do Not Respond

This scenario illustrates how to enable RADIUS authentication for both console and administrative users, but to unconditionally allow access for administrative and console users if the RADIUS server (in this case, server *r1* in server group *sg1*) does not respond. To configure unconditional authentication, Natasha sets the authentication method to **none**. She types the following commands in this order:

```
23x0# set user natasha password m@Jor
User natasha created

23x0# set radius server r1 address 192.168.253.1 key sunFLOW#$
success: change accepted.

23x0# set server group sg1 members r1
success: change accepted.

23x0# set authentication console * sg1 none
success: change accepted.

23x0# set authentication admin * sg1 none
success: change accepted.

23x0# save config
success: configuration saved.
```

Configuring and Managing Ports and VLANs

Configuring and Managing Ports 71
Configuring and Managing VLANs 88
Managing the Layer 2 Forwarding Database 96
Port and VLAN Configuration Scenario 102

Configuring and Managing Ports

You can configure and display information for the following port parameters:

- Port type
- Name
- Speed and autonegotiation
- Port state
- Power over Ethernet (PoE) state
- Load sharing

Setting the Port Type

A WSS port can be one of the following types:

- Network port. A network port is a Layer 2 switch port that connects the WSS switch to other networking devices such as switches and routers.
- AP access port. An AP access point connects the WSS to an AP access port. The port also can provide power to the AP access point. Wireless users are authenticated to the network through an AP access port.



Note. A Distributed AP, which is connected to WSS switches through intermediate Layer 2 or Layer 3 networks, does not use an AP access port. To configure for a Distributed AP, see "Configuring for a Distributed AP" on page 76 and "Configuring AP access points," on page 221.

- Wired authentication port. A wired authentication port connects the WSS switch to user devices, such as workstations, that must be authenticated to access the network.

All WSS switch ports are network ports by default. You must set the port type for ports directly connected to AP access points and to wired user stations that must be authenticated to access the network. When you change port type, WSS Software applies default settings appropriate for the port type. Table 1 lists the default settings applied for each port type. For example, the AP access point column lists default settings that WSS Software applies when you change a port type to **ap** (AP access port).

Table 1: Port Defaults Set By Port Type Change

Parameter	Port type		
	AP Access	Wired Authentication	Network
VLAN membership	Removed from all VLANs. You cannot assign an AP access point to a VLAN. WSS Software automatically assigns AP access ports to VLANs based on user traffic.	Removed from all VLANs. You cannot assign a wired authentication port to a VLAN. WSS Software automatically assigns wired authentication ports to VLANs based on user traffic.	None **Note:** If you clear a port, WSS Software resets the port as a network port but does not add the port back to any VLANs. You must explicitly add the port to the desired VLANs.
Spanning Tree Protocol (STP)	Not applicable	Not applicable	Based on the STP states of the VLANs the port is in.
802.1X	Uses authentication parameters configured for users.	Uses authentication parameters configured for users.	No authentication.
Port groups	Not applicable	Not applicable	None

Table 1: Port Defaults Set By Port Type Change (continued)

Parameter	Port type		
	AP Access	Wired Authentication	Network
IGMP snooping	Enabled as users are authenticated and join VLANs.	Enabled as users are authenticated and join VLANs.	Enabled as the port is added to VLANs.
Maximum user sessions	Not applicable	1 (one)	Not applicable

Table 2 lists how many APs you can configure on a WSS, and how many APs a switch can boot. The numbers are for directly connected and Distributed APs combined.

Table 2: Maximum APs Supported Per Switch

WSS Switch Model	Maximum That Can Be Configured	Maximum That Can Be Booted
WSS-2380	300	40, 80, or 120, depending on the license level
WSS-2370	100	40
WSS-2360	30	12
WSS-2350	8	3

WSS 2380 40 AP Software License Upgrade

The License Certificate is used to provide a single software license and its associated License Activation Key. The number of supported Access Points for your Nortel WLAN WSS 2380 will depend on the upgrade License Activation Key that is installed and active. This License upgrade supports an additional 40 APs and is only valid for use on these products running Version Software 4.0 and higher.

To enable the additional support of Access Points, you must obtain a License Activation Key from Nortel, and load the License Activation Key into WLAN WSS 2380 to activate the support.

To use this certificate to obtain a License Activation Key, follow these instructions:

1. Record the serial number of the WSS 2380 on which you wish to enable the additional Access Points. To display the switch's serial number establish a management session with the WSS 2380. Use the CLI to display the serial number, type the following command: **show version** (In the following example, the switch serial number is 1234567890:

```
2380> show version
Mobility System Software, Version 4.0.1
Copyright (c) 2002, 2003, 2004, 2005 Nortel Inc. All rights reserved
Build Information: (build#73) REL 2005-05-16 11:09:00
Model 2380
Hardware
Mainboard: version 24: revision 3: FPGA version 24
PoE board: version 1: FPGA version 6
Serial number 1234567890
```

Flash: 4.0.0.172 - md0a
Kernel: 3.0.0#253: Mon May 9 17:44:47 PDT 2005
BootLoader: 4.1/4.0.8

2. Contact Nortel using the email address to the left.
3. In the email, please include the coupon code (shown to the left) and serial number. Provide in the body of the email the contact information, including organization or company name, contact name, phone number, mailing address and e-mail address.
4. Nortel will verify the validity of the coupon code, and reply to your email with the authorization key unique for the serial number of the switch provided. Nortel will record the license activation key and associated serial number. A record of the serial number and activation key will be kept at Nortel for future reference.
5. This certificate should be stored in a secure place for future reference.

When the proper License Activation Key has been obtained, follow the instructions below to enable the WLAN WSS 2380 features:

1. Use the following command at the enable (configuration) level of the CLI to install the activation key: **set license** *activation-key*
2. Type in the entire activation key and press *enter*

   In the following example, an activation key for additional AP's is installed:
   2380# set license 3B02-D821-6C19-CE8B-F20E
   success: license accepted
3. Verify installation of the new license by typing the following command: **show license** Support for the additional AP's begins immediately. The switch does **not** need to be restarted for the upgrade to be effective.

Setting a Port for a Directly Connected AP access port

Note. Before configuring a port as an AP access port, you must use the **set system countrycode** command to set the IEEE 802.11 country-specific regulations on the WSS switch. (See "Specifying the Country of Operation" on page 248.)

To set a port for an AP access port, use the following command:

set port type ap *port-list*
model {AP2750 | AP-52 | AP-101 | AP-122 | AP-241 | AP-252 | AP-262 | AP-341 | AP-352 | AP-2330}
poe {enable | disable}
[radiotype {11a | 11b| 11g}]

You must specify a port list of one or more port numbers, the AP model number, and the PoE state. (For details about port lists, see "Port Lists" on page 41.)

AP access point models AP2750, AP-241 and AP-341 have a single radio that can be configured for 802.11a or 802.11b/g. Other AP models have two radios. One radio is always 802.11a. The other radio is 802.11b/g, but can be configured for 802.11b or 802.11g exclusively. If the country of operation specified by the **set system countrycode** command does not allow 802.11g, the default is 802.11b.



Note. All AP models except the 2330 and AP2750 have been discontinued but are still supported by the command.

AP radios configured for 802.11g also allow associations from 802.11b clients by default. To disable support for 802.11b associations, use the **set radio-profile 11g-only** command on the radio profile that contains the radio.



Note. You cannot configure any gigabit Ethernet port, or port 7 or 8 on a WSS-2360 switch, or port 1 on a WSS-2350, as an AP port. To manage an AP access point on a WSS-2380 switch, configure a Distributed AP connection on the switch. (See "Configuring for a Distributed AP" on page 76.)

AP model AP-262 requires an external antenna for the 802.11b/g radio. You must specify the Nortel antenna model. AP-3*xx* models have an internal 802.1b/g antenna as well as a connector for an external antenna, so use of an external antenna is optional on these models. The 2330 also has a connector for an optional external 802.11a antenna. To specify the antenna model, use the **set {ap | dap} radio antennatype** command. (See "Configuring the External Antenna Model" on page 274.)

To set ports 4 through 6 for AP access point model 2330 and enable PoE on the ports, type the following command:

```
23x0# set port type ap 4-6 model 2330 poe enable
This may affect the power applied on the configured ports. Would you like to
continue? (y/n) [n]y
success: change accepted.
```

To set port 7 for AP access point model AP-241, enable PoE on the port, and set the radio type to 802.11b only, type the following command:

```
23x0# set port type ap 7 model AP-241 poe enable radiotype 11b
This may affect the power applied on the configured ports. Would you like to
continue? (y/n) [n]y
success: change accepted.
```

To set port 11 for AP access point model AP-341, enable PoE on the port, and change the radio type to 802.11a, type the following command:

```
23x0# set port type ap 11 model AP-341 poe enable radiotype 11a
This may affect the power applied on the configured ports. Would you like to
continue? (y/n) [n]y
success: change accepted.
```

Note. Additional configuration is required to place an AP access point into operation. For information, see "Configuring AP access points," on page 221.

Configuring for a Distributed AP

To configure a connection for a Distributed AP (referred to as a *DAP* in the CLI), use the following command:

set dap *dap-num* **serial-id** *serial-ID*
model {MP2750 | MP-52 | MP-101 | MP-122 | MP-241 | MP-252 | MP-262 | MP-341 | MP-352 | AP-2330}
[radiotype {11a | 11b| 11g}]

The *dap-num* parameter identifies the Distributed AP connection for the AP. The range of valid connection ID numbers depends on the WSS switch model:

- For a WSS-2380, you can specify a number from 1 to 300.
- For a WSS-2370, you can specify a number from 1 to 100.
- For a WSS-2360, you can specify a number from 1 to 30.
- For a WSSR-2350, you can specify a number from 1 to 8.

For the **serial-id** parameter, specify the serial ID of the AP. The serial ID is listed on the AP case. To display the serial ID using the CLI, use the **show version details** command.

The **model** and **radiotype** parameters have the same options as they do with the **set port type ap** command. Because the WSS does not supply power to an indirectly connected AP, the **set dap** command does not use the **poe** parameter.

To configure Distributed AP connection 1 for AP model 2330 with serial-ID 0322199999, type the following command:

```
23x0# set dap 1 serial-id 0322199999 model 2330
success: change accepted.
```

To configure Distributed AP connection 2 for AP model AP-241 with serial-ID 0322188888 and radio type 802.11a, type the following command:

```
23x0# set dap 2 serial-id 0322188888 model MP-241 radiotype 11a
success: change accepted.
```

Setting a Port for a Wired Authentication User

To set a port for a wired authentication user, use the following command:

set port type wired-auth *port-list* **[tag** *tag-list***] [max-sessions** *num***]**
[auth-fall-thru {last-resort | none | web-portal}]

You must specify a port list. Optionally, you also can specify a tag-list to subdivide the port into virtual ports, set the maximum number of simultaneous user sessions that can be active on the port, and change the fallthru authentication method.

By default, one user session can be active on the port at a time.

The *fallthru* authentication type is used if the user does not support 802.1X and is not authenticated by MAC authentication. The default is none, which means the user is automatically denied access if neither 802.1X authentication or MAC authentication is successful.

To set port 17 as a wired authentication port, type the following command:

```
23x0# set port type wired-auth 17
success: change accepted
```

This command configures port 17 as a wired authentication port supporting one interface and one simultaneous user session.



Note. If clients are connected to a wired authentication port through a downstream third-party switch, the WSS switch attempts to authenticate based on any traffic coming from the switch, such as Spanning Tree Protocol (STP) BPDUs. In this case, disable repetitive traffic emissions such as STP BPDUs from downstream switches. If you want to provide a management path to a downstream switch, use MAC authentication.

Clearing a Port



Caution! When you clear a port, WSS Software ends user sessions that are using the port.

To change a port's type from AP access point or wired authentication port, you must first clear the port, then set the port type.

Clearing a port removes all the port's configuration settings and resets the port as a network port.

- If the port is an AP access port, clearing the port disables PoE and 802.1X authentication.
- If the port is a wired authenticated port, clearing the port disables 802.1X authentication.
- If the port is a network port, the port must first be removed from all VLANs, which removes the port from all spanning trees, load-sharing port groups, and so on.



Note. A cleared port is not placed in any VLANs, not even the default VLAN (VLAN 1).

To clear a port, use the following command:

clear port type *port-list*

For example, to clear the port-related settings from port 5 and reset the port as a network port, type the following command:

```
23x0# clear port type 5
Thismaydisruptcurrentlyauthenticatedusers.Areyousure?(y/n)[n]y
success: change accepted.
```

Clearing a Distributed AP



Caution! When you clear a Distributed AP, WSS Software ends user sessions that are using the AP.

To clear a Distributed AP, use the following command:

clear dap *dap-num*

Configuring a Port Name

Each WSS switch port has a number but does not have a name by default.

Setting a Port Name

To set a port name, use the following command:

set port *port* **name** *name*

You can specify only a single port number with the command.

To set the name of port 17 to *adminpool*, type the following command:

```
23x0# set port 17 name adminpool
success: change accepted.
```



Note. To avoid confusion, Nortel recommends that you do not use numbers as port names.

Removing a Port Name

To remove a port name, use the following command:

clear port *port-list* **name**

Configuring Interface Preference on a Dual-Interface Gigabit Ethernet Port (WSS-400 only)

The gigabit Ethernet ports on an WSS-2380 switch have two physical interfaces: a 1000BASE-TX copper interface and a 1000BASE-SX or 1000BASE-LX fiber interface. The copper interface is provided by a built-in RJ-45 connector. The fiber interface is optional and requires insertion of a Gigabit interface converter (GBIC).

Only one interface can be active on a port. By default, WSS Software prefers the GBIC (fiber) interface. You can configure a port to prefer the RJ-45 (copper) interface instead.

If you set the preference to RJ-45 on a port that already has an active fiber link, WSS Software immediately changes the link to the copper interface.

To configure a port to prefer the copper interface, use the following command:

set port preference *port-list* **rj45**

To remove the preference setting from a port so that GBIC (fiber) is preferred again, use the following command:

clear port preference *port-list*

To display preference settings, use the following command:

show port preference [*port-list*]

To set the preference of port 2 on an WSS-2380 switch to copper and verify the change, type the following commands:

```
WSS-2380# set port preference 2 rj45

WSS-2380# show port preference
Port  Preference
============================================================
   1  GBIC
   2  RJ45
   3  GBIC
   4  GBIC
```

Configuring Port Operating Parameters

Autonegotiation is enabled by default on an WSS switch's 10/100 Ethernet ports and gigabit Ethernet ports.

Note. All ports on the WSS-2370 and WSS-2380 switches support full-duplex operating mode only. They do not support half-duplex operation. Ports on the WSS-2360 switch support half-duplex and full-duplex operation.

You can configure the following port operating parameters:

- Speed
- Autonegotiation
- Port state
- PoE state

You also can toggle a port's administrative state and PoE setting off and back on to reset the port.

10/100 Ports—Autonegotiation and Port Speed

WSS 10/100 Ethernet ports use autonegotiation by default to determine the appropriate port speed.

To explicitly set the port speed of a 10/100 port, use the following command:

set port speed *port-list* **{10 | 100 | auto}**

Note. If you explicitly set the port speed (by selecting an option other than **auto**) of a 10/100 Ethernet port, the operating mode is set to full-duplex.

To set the port speed on ports 1, 7 through 11, and 14 to 10 Mbps, type the following command:

```
23x0# set port speed 1,7-11,14 10
```

Gigabit Ports—Autonegotiation and Flow Control

WSS gigabit ports use autonegotiation by default to determine capabilities for 802.3z flow control parameters. The gigabit ports can respond to IEEE 802.3z flow control packets. Some devices use this capability to prevent packet loss by temporarily pausing data transmission.

To disable flow control negotiation on an WSS gigabit port, use the following command:

set port negotiation *port-list* **{enable | disable}**

10/100 Ethernet Ports—Full-Duplex-Only Operation (WSS-2370 only)

WSS-2360 10/100 Ethernet ports support half-duplex and full-duplex operation.

WSS-2370 10/100 Ethernet ports do not support half-duplex operation. As a result, there are restrictions when WSS-20 10/100 Ethernet ports are interoperating with other vendors' devices. For a link to occur, the autonegotiation settings on

a WSS-2370 switch port and the device at the other end of the link must be the same. In addition, the other device must support full-duplex operation. When autonegotiation is enabled on a WSS-2370 switch port, the port advertises support for full-duplex mode only. Table 3 lists the supported configurations.

Table 3: Supported 10/100 Ethernet Speeds and Operating Modes for WSS-2370 Switch

		WSS-2370 Setting		
		100 Mbps Full-duplex	**10 Mbps Full-duplex**	**Autonegotiation**
Other Device's Setting	**100 Mbps Full-duplex**	100 Mbps full-duplex	Not supported	Not supported
	10 Mbps Full-duplex	Not supported	10 Mbps full-duplex	Not supported
	100 Mbps Half-duplex	Not supported	Not supported	Not supported
	10 Mbps Half-duplex	Not supported	Not supported	Not supported
	Autonegotiation	Not supported	Not supported	100 Mbps full-duplex

Disabling or Reenabling a Port

All ports are enabled by default. To administratively disable a port, use the following command:

set port {**enable** | **disable**} *port-list*

A port that is administratively disabled cannot send or receive packets. This command does not affect the link state of the port.

Disabling or Reenabling Power over Ethernet

Power over Ethernet (PoE) supplies DC power to a device connected to an AP access port. The PoE state depends on whether you enable or disable PoE when you set the port type. (See "Setting the Port Type" on page 72.)



Caution! Use the WSS switch's PoE only to power Nortel AP access ports. If you enable PoE on ports connected to other devices, damage can result.



Note. PoE is supported only on 10/100 Ethernet ports. PoE is not supported on any gigabit Ethernet ports, or on ports 7 and 8 on an WSS-2360 switch.

To change the PoE state on a port, use the following command:

set port poe *port-list* **enable** | **disable**

Resetting a Port

You can reset a port by toggling its link state and PoE state. WSS Software disables the port's link and PoE (if applicable) for at least one second, then reenables them. This feature is useful for forcing an AP access point that is connected to two WSS switches to reboot using the port connected to the other switch.

To reset a port, use the following command:

reset port *port-list*

Displaying Port Information

You can use CLI commands to display the following port information:

- Port configuration and status
- PoE state
- Port statistics

You also can configure WSS Software to display and regularly update port statistics in a separate window.

Displaying Port Configuration and Status

To display port configuration and status information, use the following command:

show port status [*port-list*]

To display information for all ports, type the following command:

```
23x0# show port status
Port  Name              Admin  Oper   Config     Actual    Type        Media
=============================================================================
   1  1                 up     up     auto       100/full  network     10/100BaseTx
   2  2                 up     down   auto                 network     10/100BaseTx
   3  3                 up     down   auto                 network     10/100BaseTx
   4  4                 up     down   auto                 network     10/100BaseTx
   5  5                 up     down   auto                 network     10/100BaseTx
   6  6                 up     down   auto                 network     10/100BaseTx
   7  7                 up     down   auto                 network     10/100BaseTx
   8  8                 up     down   auto                 network     10/100BaseTx
   9  9                 up     up     auto       100/full  ap          10/100BaseTx
  10  10                up     up     auto       100/full  network     10/100BaseTx
  11  11                up     down   auto                 network     10/100BaseTx
  12  12                up     down   auto                 network     10/100BaseTx
  13  13                up     down   auto                 network     10/100BaseTx
  14  14                up     down   auto                 network     10/100BaseTx
  15  15                up     down   auto                 network     10/100BaseTx
  16  16                up     down   auto                 network     10/100BaseTx
  17  17                up     down   auto                 network     10/100BaseTx
  18  18                up     down   auto                 network     10/100BaseTx
  19  19                up     down   auto                 network     10/100BaseTx
  20  20                up     down   auto                 network     10/100BaseTx
  21  21                up     down   auto                 network     no connector
  22  22                up     down   auto                 network     no connector
```

In this example, three of the switch's ports, 1, 9, and 10, have an operational status of *up*, indicating the links on the ports are available. Ports 1 and 10 are network ports. Port 9 is an AP access port.

(For more information about the fields in the output, see the *Nortel WLAN Security Switch 2300 Software Command Reference*.)

Displaying PoE State

To display the PoE state of a port, use the following command:

show port poe [*port-list*]

To display PoE information for ports 7 and 9, type the following command:

```
23x0# show port poe 7,9
                        Link      Port    PoE         PoE
Port  Name              Status    Type    config      Draw
=============================================================
   7  7                 down      AP      disabled    off
   9  9                 up        AP      enabled     1.44
```

In this example, PoE is disabled on port 7 and enabled on port 9. The AP access point connected to port 9 is drawing 1.44 W of power from the WSS.

(For more information about the fields in the output, see the *Nortel WLAN Security Switch 2300 Software Command Reference*.)

Displaying Port Statistics

To display port statistics, use the following command:

show port counters [octets | packets | receive-errors | transmit-errors | collisions | receive-etherstats | transmit-etherstats] [port *port-list*]

You can specify one statistic type with the command. For example, to display octet statistics for port 3, type the following command:

```
23x0# show port counters octets port 3
Port   Status                      Rx Octets                      Tx Octets
=============================================================================
   3   Up                          27965420                       34886544
```

(For information about the fields in the output, see the *Nortel WLAN Security Switch 2300 Software Command Reference*.)



Note. To display all types of statistics with the same command, use the **monitor port counters** command. (See "Monitoring Port Statistics" on page 85.)

Clearing Statistics Counters

To clear all port statistics counters, use the following command:

clear port counters

The counters begin incrementing again, starting from 0.

Monitoring Port Statistics

You can display port statistics in a format that continually updates the counters. When you enable monitoring of port statistics, WSS Software clears the CLI session window and displays the statistics at the top of the window. WSS Software refreshes the statistics every 5 seconds. This interval cannot be configured.

To monitor port statistics, use the following command:

monitor port counters [octets | packets | receive-errors | transmit-errors | collisions | receive-etherstats | transmit-etherstats]

Statistics types are displayed in the following order by default:

- Octets
- Packets
- Receive errors
- Transmit errors
- Collisions
- Receive Ethernet statistics
- Transmit Ethernet statistics

Each type of statistic is displayed separately. Press the Spacebar to cycle through the displays for each type.

If you use an option to specify a statistic type, the display begins with that statistic type. You can use one statistic option with the command.

Use the keys listed in Table 4 to control the monitor display.

Table 4: Key Controls for Monitor Port Counters Display

Key	Effect on monitor display
Spacebar	Advances to the next statistics type.
Esc	Exits the monitor. WSS Software stops displaying the statistics and displays a new command prompt.
c	Clears the statistics counters for the currently displayed statistics type. The counters begin incrementing again.

To monitor port statistics beginning with octet statistics (the default), type the following command:

```
23x0# monitor port counters
```

As soon as you press Enter, WSS Software clears the window and displays statistics at the top of the window. In this example, the octet statistics are displayed first.

```
Port   Status                        Rx Octets                          Tx Octets
================================================================================
    1  Up                          27965420                          34886544
...
```

To cycle the display to the next set of statistics, press the Spacebar. In this example, packet statistics are displayed next:

```
Port   Status    Rx Unicast    Rx NonUnicast      Tx Unicast    Tx NonUnicast
================================================================================
    1  Up            54620            62144           68318            62556
...
```

(For information about the fields in the output, see the *Nortel WLAN Security Switch 2300 Software Command Reference*.)

Configuring Load-Sharing Port Groups

A port group is a set of physical ports that function together as a single link and provide load sharing and link redundancy. Only network ports can participate in a port group.

You can configure up to 16 ports in a port group, in any combination of ports. The port numbers do not need to be contiguous and you can use 10/100 Ethernet ports and gigabit Ethernet ports in the same port group.

Load Sharing

An WSS switch balances the port group traffic among the group's physical ports by assigning traffic flows to ports based on the traffic's source and destination MAC addresses. The switch assigns a traffic flow to an individual port and uses the same port for all subsequent traffic for that flow.

Link Redundancy

A port group ensures link stability by providing redundant connections for the same link. If an individual port in a group fails, the WSS reassigns traffic to the remaining ports. When the failed port starts operating again, the WSS switch begins using it for new traffic flows. Traffic that belonged to the port before it failed continues to be assigned to other ports.

Configuring a Port Group

To configure a port group, use the following command:

set port-group name *group-name port-list* **mode {on | off}**

Enter a name for the group and the ports contained in the group.

The **mode** parameter adds or removes ports for a group that is already configured. To modify a group:

- Adding ports—Enter the ports you want to add, then enter **mode on**.
- Removing ports—Enter the ports you want to remove, then enter **mode off**.

To configure a port group named *server1* containing ports 1 through 5 and enable the link, type the following command:

```
23x0# set port-group name server1 1-5 mode on
success: change accepted.
```

After you configure a port group, you can use the port group name with commands that change Layer 2 configuration parameters to apply configuration changes to all ports in the port group. For example, Spanning Tree Protocol (STP) and VLAN membership changes affect the entire port group instead of individual ports. When you make Layer 2 configuration changes, you can use a port group name in place of the port list. Ethernet port statistics continue to apply to individual ports, not to port groups.

To configure a port group named *server2* containing ports 15 and 17 and add the ports to the *default* VLAN, type the following commands:

```
23x0# set port-group name server2 15,17 mode on
success: change accepted.

23x0# set vlan default port server2
success: change accepted.
```

To verify the configuration change, type the following command:

```
23x0# show vlan config
                          Admin  VLAN  Tunl                      Port
VLAN Name            Status State Affin Port           Tag   State
---- ------------------ ------ ----- ----- -------------- ----- -----
   1 default            Up     Up        5
                                             server2           none  Up
```

To indicate that the ports are configured as a port group, the **show vlan config** output lists the port group name instead of the individual port numbers.

Removing a Port Group

To remove a port group, use the following command:

clear port-group name *name*

Displaying Port Group Information

To display port group information, use the following command:

show port-group [**all** | **name** *group-name*]

To display the configuration and status of port group *server2*, type the following command:

```
23x0# show port-group name server2
Port group: server2 is up
        Ports:  15, 17
```

Interoperating with Cisco Systems EtherChannel

Load-sharing port groups are interoperable with Cisco Systems EtherChannel capabilities. To configure a Cisco Catalyst switch to interoperate with a Nortel WSS, use the following command on the Catalyst switch:

set port channel *port-list* **mode on**

Configuring and Managing VLANs

Note. The CLI commands in this chapter configure VLANs on WSS network ports. The commands do not configure VLAN membership for wireless or wired authentication users. To assign a user to a VLAN, configure the RADIUS Tunnel-Private-Group-ID attribute or the VLAN-Name vendor specific attribute (VSA) for that user. (For more information, see "Configuring AAA for Network Users," on page 401.)

Understanding VLANs in Nortel WSS Software

A virtual LAN (VLAN) is a Layer 2 broadcast domain that can span multiple wired or wireless LAN segments. Each VLAN is a separate logical network and, if you configure IP interfaces on the VLANs, WSS Software treats each VLAN as a separate IP subnet.

Only network ports can be preconfigured to be members of one or more VLANs. You configure VLANs on a WSS's network ports by configuring them on the switch itself. You configure a VLAN by assigning a name and network ports to the VLAN. Optionally, you can assign VLAN tag values on individual network ports. You can configure multiple VLANs on a WSS's network ports. Optionally, each VLAN can have an IP address.

VLANs are not configured on AP access ports or wired authentication ports, because the VLAN membership of these types of ports is determined dynamically through the authentication and authorization process. Users who require authentication connect through WSS switch ports that are configured for AP access ports or wired authentication access. Users are assigned to VLANs automatically through authentication and authorization mechanisms such as 802.1X.

By default, none of an WSS switch's ports are in VLANs. A switch cannot forward traffic on the network until you configure VLANs and add network ports to those VLANs.



Note. A wireless client cannot join a VLAN if the physical network ports on the WSS switch in the VLAN are down. However, a wireless client that is already in a VLAN whose physical network ports go down remains in the VLAN even though the VLAN is down.

VLANs, IP Subnets, and IP Addressing

Generally, VLANs are equivalent to IP subnets. If a WSS is connected to the network by only one IP subnet, the switch must have at least one VLAN configured. Optionally, each VLAN can have its own IP address. However, no two IP addresses on the switch can belong to the same IP subnet.

You must assign the system IP address to one of the VLANs, for communications between WSSs and for unsolicited communications such as SNMP traps and RADIUS accounting messages. Any IP address configured on a WSS can be used for management access unless explicitly restricted. (For more information about the system IP address, see "Configuring and Managing IP Interfaces and Services," on page 107.)

Users and VLANs

When a user successfully authenticates to the network, the user is assigned to a specific VLAN. A user remains associated with the same VLAN throughout the user's session on the network, even when roaming from one WSS to another within the Mobility Domain.

You assign a user to a VLAN by setting one of the following attributes on the RADIUS servers or in the local user database:

- Tunnel-Private-Group-ID—This attribute is described in RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*.

- VLAN-Name—This attribute is a Nortel vendor-specific attribute (VSA).

Note. You cannot configure the Tunnel-Private-Group-ID attribute in the local user database.

Specify the VLAN name, not the VLAN number. The examples in this chapter assume the VLAN is assigned on a RADIUS server with either of the valid attributes. (For more information, see "Configuring AAA for Network Users," on page 401.)

VLAN Names

To create a VLAN, you must assign a name to it. VLAN names must be globally unique across a Mobility Domain to ensure the intended user connectivity as determined through authentication and authorization.

Every VLAN on a WSS has both a VLAN name, used for authorization purposes, and a VLAN number. VLAN numbers can vary uniquely for each WSS switch and are not related to 802.1Q tag values.

You cannot use a number as the first character in a VLAN name.

Roaming and VLANs

WSS switches in a Mobility Domain contain a user's traffic within the VLAN that the user is assigned to. For example, if you assign a user to VLAN *red*, the WSSs in the Mobility Domain contain the user's traffic within VLAN *red* configured on the switches.

The WSS switch through which a user is authenticated is not required to be a member of the VLAN the user is assigned to. You are not required to configure the VLAN on all WSSs in the Mobility Domain. When a user roams to a switch that is not a member of the VLAN the user is assigned to, the switch can tunnel traffic for the user through another switch that is a member of the VLAN. The traffic can be of any protocol type. (For more information about Mobility Domains, see "Configuring and Managing Mobility Domain Roaming," on page 175.)

Note. Because the *default* VLAN (VLAN 1) might not be in the same subnet on each switch, Nortel recommends that you do not rename the default VLAN or use it for user traffic. Instead, configure other VLANs for user traffic.

Traffic Forwarding

An WSS switch switches traffic at Layer 2 among ports in the same VLAN. For example, suppose you configure ports 4 and 5 to belong to VLAN 2 and ports 6 and 7 to belong to VLAN 3. As a result, traffic between port 4 and port 5 is switched, but traffic between port 4 and port 6 is not switched and needs to be routed by an external router.

802.1Q Tagging

The tagging capabilities of the WSS are very flexible. You can assign 802.1Q tag values on a per-VLAN, per-port basis. The same VLAN can have different tag values on different ports. In addition, the same tag value can be used by different VLANs but on different network ports.

If you use a tag value, Nortel recommends that you use the same value as the VLAN number. WSS Software does not require the VLAN number and tag value to be the same, but some other vendors' devices do.



Note. Do not assign the same VLAN multiple times using different tag values to the same network port. Although WSS Software does not prohibit you from doing so, the configuration is not supported.

Tunnel Affinity

WSS switches configured as a Mobility Domain allow users to roam seamlessly across AP access ports and even across WSSs. Although a switch that is not a member of a user's VLAN cannot directly forward traffic for the user, the switch can tunnel the traffic to another WSS switch that is a member of the user's VLAN.

If the WSS that is not in the user's VLAN has a choice of more than one other WSS switch through which to tunnel the user's traffic, the switch selects the other switch based on an affinity value. This is a numeric value that each WSS switch within a Mobility Domain advertises, for each of its VLANs, to all other switches in the Mobility Domain. A switch outside the user's VLAN selects the other operational switch that has the highest affinity value for the user's VLAN to forward traffic for the user.

If more than one WSS switch has the highest affinity value, WSS Software randomly selects one of the switches for the tunnel.

Configuring a VLAN

You can configure the following VLAN parameters:

- VLAN number
- VLAN name
- Port list (the ports in the VLAN)
- Per-port tag value (an 802.1Q value representing a virtual port in the VLAN)
- Tunnel affinity (a value that influences tunneling connections for roaming)

Creating a VLAN

To create a VLAN, use the following command:

set vlan *vlan-num* **name** *name*

Specify a VLAN number from 2 to 4095, and specify a name up to 16 alphabetic characters long.

You cannot use a number as the first character in a VLAN name. Nortel recommends that you do not use the same name with different capitalizations for VLANs or ACLs. For example, do not configure two separate VLANs with the names *red* and *RED*.



Note. Nortel recommends that you do not use the name *default*. This name is already used for VLAN 1. Nortel also recommends that you do not rename the default VLAN.

You must assign a name to a VLAN before you can add ports to the VLAN. You can configure the name and add ports with a single **set vlan** command or separate **set vlan** commands.

Once you assign a VLAN number to a VLAN, you cannot change the number. However, you can change a VLAN's name.

For example, to assign the name *red* to VLAN 2, type the following command:

```
23x0# set vlan 2 name red
```

After you create a VLAN, you can use the VLAN number or the VLAN name in commands. In addition, the VLAN name appears in CLI and WLAN Management Software displays.

Adding Ports to a VLAN

To add a port to a VLAN, use the following command:

set vlan *vlan-id* **port** *port-list* [**tag** *tag-value*]

You can specify a tag value from 1 through 4095.



Note. WSS Software does not remove a port from other VLANs when you add the port to a new VLAN. If a new VLAN causes a configuration conflict with an older VLAN, remove the port from the older VLAN before adding the port to the new VLAN.

For example, to add ports 9 through 11 and port 21 to VLAN *red*, type the following command:

```
23x0# set vlan red port 9-11,21
success: change accepted.
```

Optionally, you also can specify a tag value to be used on trunked 802.1Q ports.

To assign the name *marigold* to VLAN 4, add ports 12 through 19 and port 22, and assign tag value 11 to port 22, type the following commands:

```
23x0# set vlan 4 name marigold port 12-19
success: change accepted.

23x0# set vlan 4 name marigold port 22 tag 11
success: change accepted.
```

Removing an Entire VLAN or a VLAN Port

To remove an entire VLAN or a specific port and tag value from a VLAN, use the following command:

clear vlan *vlan-id* [**port** *port-list* [**tag** *tag-value*]]



Caution! When you remove a VLAN, WSS Software completely removes the VLAN from the configuration and also removes all configuration information that uses the VLAN. If you want to remove only a specific port from the VLAN, make sure you specify the port number in the command.

The **clear vlan** command with a VLAN ID but without a port list or tag value clears all ports and tag values from the VLAN.

To remove port 21 from VLAN *red*, type the following command:

```
23x0# clear vlan red port 21
Thismaydisruptuserconnectivity.Doyouwishtocontinue?(y/n)[n]y
success: change accepted.
```

To clear port 13, which uses tag value 11, from VLAN *marigold*, type the following command:

```
23x0# clear vlan marigold port 13 tag 11
Thismaydisruptuserconnectivity.Doyouwishtocontinue?(y/n)[n]y
success: change accepted.
```

To completely remove VLAN *ecru*, type the following command:

```
23x0# clear vlan ecru
Thismaydisruptuserconnectivity.Doyouwishtocontinue?(y/n)[n]y
success: change accepted.
```



Note. You cannot remove the default VLAN (VLAN 1). However, you can add and remove ports. You can also rename the default VLAN, but Nortel recommends against it.

Changing Tunneling Affinity

To change the tunneling affinity, use the following command:

set vlan *vlan-id* **tunnel-affinity** *num*

Specify a value from 1 through 10. The default is 5.

Displaying VLAN Information

To display VLAN configuration information, use the following command:

show vlan config [*vlan-id*]

To display information for VLAN *burgundy*, type the following command:

```
23x0# show vlan config burgundy
                    Admin  VLAN  Tunl                      Port
VLAN Name           Status State Affin Port          Tag   State
---- -------------------- ------ ----- ------------------ ----- -----
   2 burgundy          Up     Up        5
                                      2                 none Up
                                      3                 none Up
                                      4                 none Up
                                      6                 none Up
                                      11                none Up
```

Note. The display can include AP access ports and wired authentication ports, because WSS Software dynamically adds these ports to a VLAN when handling user traffic for the VLAN.

(For information about the fields in the output, see the *Nortel WLAN Security Switch 2300 Software Command Reference*.)

Managing the Layer 2 Forwarding Database

An WSS switch uses a Layer 2 forwarding database (FDB) to forward traffic within a VLAN. The entries in the forwarding database map MAC addresses to the physical or virtual ports connected to those MAC addresses within a particular VLAN. To forward a packet to another device in a VLAN, the WSS switch searches the forwarding database for the packet's destination MAC address, then forwards the packet out the port associated with the MAC address.

Types of Forwarding Database Entries

The forwarding database can contain the following types of entries:

- Dynamic—A dynamic entry is a temporary entry that remains in the database only until the entry is no longer used. By default, a dynamic entry ages out if it remains unused for 300 seconds (5 minutes). All dynamic entries are removed if the WSS is powered down or rebooted.
- Static—A static entry does not age out, regardless of how often the entry is used. However, like dynamic entries, static entries are removed if the WSS is powered down or rebooted.
- Permanent—A permanent entry does not age out, regardless of how often the entry is used. In addition, a permanent entry remains in the forwarding database even following a reboot or power cycle.

How Entries Enter the Forwarding Database

An entry enters the forwarding database in one of the following ways:

- Learned from traffic received by the WSS —When the WSS receives a packet, the switch adds the packet's source MAC address to the forwarding database if the database does not already contain an entry for that MAC address.
- Added by the system administrator—You can add static and permanent unicast entries to the forwarding database. (You cannot add a multicast or broadcast address as a permanent or static forwarding database entry.)
- Added by the WSS itself—For example, the authentication protocols can add entries for wired and wireless authentication users. The WSS also adds any static entries added by the system administrator and saved in the configuration file.

Displaying Forwarding Database Information

You can display the forwarding database size and the entries contained in the database.

Displaying the Size of the Forwarding Database

To display the number of entries contained in the forwarding database, use the following command:

show fdb count {perm | static | dynamic} [vlan *vlan-id***]**

For example, to display the number of dynamic entries that the forwarding database contains, type the following command:

```
23x0# show fdb count dynamic
Total Matching Entries = 2
```

Displaying Forwarding Database Entries

To display the entries in the forwarding database, use either of the following commands:

show fdb [_mac-addr-wildcard_ **[vlan** _vlan-id_**]]**

show fdb {perm | static | dynamic | system | all} [port _port-list_ **| vlan** _vlan-id_**]**

The *mac-addr-wildcard* parameter can be an individual address, or a portion of an address with the asterisk (*) wildcard character representing from 1 to 5 bytes. The wildcard allows the parameter to indicate a list of MAC addresses that match all the characters except the asterisk.

Use a colon between each byte in the address (for example, **11:22:33:aa:bb:cc** or **11:22:33:***). You can enter the asterisk (*) at the beginning or end of the address as a wildcard, on any byte boundary.

To display all entries in the forwarding database, type the following command:

```
23x0# show fdb all
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG  Dest MAC/Route Des [CoS]  Destination Ports        [Protocol Type]
---- ---- ------------------ -----  ---------------------------------------
   1      00:01:97:13:0b:1f              1                        [ALL]
   1      aa:bb:cc:dd:ee:ff      *       3                        [ALL]
   1      00:0b:0e:02:76:f5              1                        [ALL]
Total Matching FDB Entries Displayed = 3
```

To display all entries that begin with 00, type the following command:

```
23x0# show fdb 00:*
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG  Dest MAC/Route Des [CoS]  Destination Ports        [Protocol Type]
---- ---- ------------------ -----  ---------------------------------------
   1      00:01:97:13:0b:1f              1                        [ALL]
   1      00:0b:0e:02:76:f5              1                        [ALL]
Total Matching FDB Entries Displayed = 2
```

(For information about the fields in the output, see the *Nortel WLAN Security Switch 2300 Software Command Reference*.)

Adding an Entry to the Forwarding Database

To add an entry to the forwarding database, use the following command:

set fdb {**perm** | **static**} *mac-addr* **port** *port-list* **vlan** *vlan-id* [**tag** *tag-value*]

To add a permanent entry for MAC address 00:bb:cc:dd:ee:ff on ports 3 and 5 in VLAN *blue*, type the following command:

```
23x0# set fdb perm 00:bb:cc:dd:ee:ff port 3,5 vlan blue
success: change accepted.
```

To add a static entry for MAC address 00:2b:3c:4d:5e:6f on port 1 in the *default* VLAN, type the following command:

```
23x0# set fdb static 00:2b:3c:4d:5e:6f port 1 vlan default
success: change accepted.
```

Removing Entries from the Forwarding Database

To remove an entry from the forwarding database, use the following command:

clear fdb {**perm** | **static** | **dynamic** | **port** *port-list*} [**vlan** *vlan-id*] [**tag** *tag-value*]

To clear all dynamic forwarding database entries that match all VLANs, type the following command:

```
23x0# clear fdb dynamic
success: change accepted.
```

To clear all dynamic forwarding database entries that match ports 3 and 5, type the following command:

```
23x0# clear fdb port 3,5
success: change accepted.
```

Configuring the Aging Timeout Period

The aging timeout period specifies how long a dynamic entry can remain unused before the software removes the entry from the database.

You can change the aging timeout period on an individual VLAN basis. You can change the timeout period to a value from 0 through 1,000,000 seconds. The default aging timeout period is 300 seconds (5 minutes). If you change the timeout period to 0, aging is disabled.

Displaying the Aging Timeout Period

To display the current setting of the aging timeout period, use the following command:

show fdb agingtime [**vlan** *vlan-id*]

For example, to display the aging timeout period for all configured VLANs, type the following command:

```
23x0# show fdb agingtime
VLAN 2 aging time = 300 sec
VLAN 1 aging time = 300 sec
```

Changing the Aging Timeout Period

To change the aging timeout period, use the following command:

set fdb agingtime *vlan-id* **age** *seconds*

For example, to set the aging timeout period for VLAN 2 to 600 seconds, type the following command:

```
23x0# set fdb agingtime 2 age 600
success: change accepted.
```

Port and VLAN Configuration Scenario

This scenario assigns names to ports, and configures AP access ports, wired authentication ports, a load-sharing port group, and VLANs.

1. Assign names to ports to identify their functions, and verify the configuration change. Type the following commands:

```
23x0# set port 1 name WSS_mgmt
success: change accepted.

23x0# set port 2 name finance
success: change accepted.

23x0# set port 3 name accounting
success: change accepted.

23x0# set port 4 name shipping
success: change accepted.

23x0# set port 5 name lobby
```

```
success: change accepted.
```

23x0# **set port 6 name conf_room1**
```
success: change accepted.
```

23x0# **set port 7 name conf_room2**
```
success: change accepted.
```

23x0# **set port 8-13 name manufacturing**
```
success: change accepted.
```

23x0# **set port 14-18 name rsrch_dev**
```
success: change accepted.
```

23x0# **set port 19-20 name mobility**
```
success: change accepted.
```

23x0# **set port 21,22 name backbone**
```
success: change accepted.
```

23x0# **show port status**

Port	Name	Admin	Oper	Config	Actual	Type	Media
1	WSS_mgmt	up	up	auto	100/full	network	10/100BaseTx
2	finance	up	down	auto		network	10/100BaseTx
3	accounting	up	down	auto		network	10/100BaseTx
4	shipping	up	down	auto		network	10/100BaseTx
5	lobby	up	down	auto		network	10/100BaseTx
6	conf_room1	up	down	auto		network	10/100BaseTx
7	conf_room2	up	down	auto		network	10/100BaseTx
8	manufacturing	up	down	auto		network	10/100BaseTx
9	manufacturing	up	down	auto		network	10/100BaseTx
10	manufacturing	up	down	auto		network	10/100BaseTx
11	manufacturing	up	down	auto		network	10/100BaseTx
12	manufacturing	up	down	auto		network	10/100BaseTx
13	manufacturing	up	down	auto		network	10/100BaseTx
14	rsrch_dev	up	down	auto		network	10/100BaseTx
15	rsrch_dev	up	down	auto		network	10/100BaseTx
16	rsrch_dev	up	down	auto		network	10/100BaseTx
17	rsrch_dev	up	down	auto		network	10/100BaseTx
18	rsrch_dev	up	down	auto		network	10/100BaseTx
19	mobility	up	up	auto	100/full	network	10/100BaseTx
20	mobility	up	up	auto	100/full	network	10/100BaseTx
21	backbone	up	down	auto		network	
22	backbone	up	down	auto		network	

2 Configure the country code for operation in the US and verify the configuration change. Type the following commands:

23x0# **set system countrycode US**
```
success: change accepted.
```

23x0# **show system**
```
================================================================================
 Product Name:       WSS-20
 System Name:        WSS-20
 System Countrycode: US
 System Location:
```

```
System Contact:
System IP:          0.0.0.0
System MAC:         00:0B:0E:00:04:0C
License:            unlimited
================================================================================
Boot Time:          2000-03-18 22:59:19
Uptime:                 0 days 00:13:45
================================================================================
Fan status:  fan1 OK fan2 OK fan3 OK
Temperature: temp1 ok  temp2 ok  temp3 ok
PSU Status:  Lower Power Supply DC ok AC ok  Upper Power Supply missing
Memory:      156.08/496.04 (31%)
Total Power Over Ethernet : 0.000
================================================================================
```

3 Configure ports 2 through 16 for connection to AP access point model 2330 and verify the configuration changes. Type the following commands:

```
23x0# set port type ap 2-16 model 2330 poe enable
Thismayaffectthepowerappliedontheconfiguredports.Wouldyouliketocontinue?(y/n)[n]y
success: change accepted.

23x0# show port status
Port  Name             Admin  Oper    Config    Actual     Type       Media
================================================================================
   1  WSS_mgmt          up     up      auto      100/full  network    10/100BaseTx
   2  finance          up     up      auto      100/full  ap         10/100BaseTx
   3  accounting       up     up      auto      100/full  ap         10/100BaseTx
   4  shipping         up     up      auto      100/full  ap         10/100BaseTx
   5  lobby            up     up      auto      100/full  ap         10/100BaseTx
   6  conf_room1       up     up      auto      100/full  ap         10/100BaseTx
   7  conf_room2       up     up      auto      100/full  ap         10/100BaseTx
   8  manufacturing    up     up      auto      100/full  ap         10/100BaseTx
   9  manufacturing    up     up      auto      100/full  ap         10/100BaseTx
  10  manufacturing    up     up      auto      100/full  ap         10/100BaseTx
  11  manufacturing    up     up      auto      100/full  ap         10/100BaseTx
  12  manufacturing    up     up      auto      100/full  ap         10/100BaseTx
  13  manufacturing    up     up      auto      100/full  ap         10/100BaseTx
  14  rsrch_dev        up     up      auto      100/full  ap         10/100BaseTx
  15  rsrch_dev        up     up      auto      100/full  ap         10/100BaseTx
  16  rsrch_dev        up     up      auto      100/full  ap         10/100BaseTx
  17  rsrch_dev        up     down    auto                network    10/100BaseTx
  18  rsrch_dev        up     down    auto                network    10/100BaseTx
  19  mobility         up     up      auto      100/full  network    10/100BaseTx
  20  mobility         up     up      auto      100/full  network    10/100BaseTx
  21  backbone         up     down    auto                network
  22  backbone         up     down    auto                network

23x0# show port poe
                     Link     Port    PoE       PoE
Port  Name           Status   Type    config    Draw(Watts)
================================================================================
   1  WSS_mgmt          up       -     disabled  off
   2  finance          up       AP    enabled    7.04
   3  accounting       up       AP    enabled    7.04
   4  shipping         up       AP    enabled    7.04
   5  lobby            up       AP    enabled    7.04
   6  conf_room1       up       AP    enabled    7.04
   7  conf_room2       up       AP    enabled    7.04
```

```
  8  manufacturing   up       AP    enabled    7.04
  9  manufacturing   up       AP    enabled    7.04
 10  manufacturing   up       AP    enabled    7.04
 11  manufacturing   up       AP    enabled    7.04
 12  manufacturing   up       AP    enabled    7.04
 13  manufacturing   up       AP    enabled    7.04
 14  rsrch_dev       up       AP    enabled    7.04
 15  rsrch_dev       up       AP    enabled    7.04
 16  rsrch_dev       up       AP    enabled    7.04
 17  rsrch_dev       down     -     disabled  off
 18  rsrch_dev       down     -     disabled  off
 19  mobility        down     -     disabled  off
 20  mobility        down     -     disabled  off
 21  backbone        down     -     -         invalid
 22  backbone        down     -     -         invalid
```

4 Configure ports 17 and 18 as wired authentication ports and verify the configuration change. Type the following commands:

```
23x0# set port type wired-auth 17,18
success: change accepted
```

```
23x0# show port status
Port  Name            Admin  Oper    Config    Actual     Type        Media
================================================================================
   1  WSS_mgmt         up     up      auto      100/full  network     10/100BaseTx
   2  finance         up     up      auto      100/full  ap          10/100BaseTx
   3  accounting      up     up      auto      100/full  ap          10/100BaseTx
   4  shipping        up     up      auto      100/full  ap          10/100BaseTx
   5  lobby           up     up      auto      100/full  ap          10/100BaseTx
   6  conf_room1      up     up      auto      100/full  ap          10/100BaseTx
   7  conf_room2      up     up      auto      100/full  ap          10/100BaseTx
   8  manufacturing   up     up      auto      100/full  ap          10/100BaseTx
   9  manufacturing   up     up      auto      100/full  ap          10/100BaseTx
  10  manufacturing   up     up      auto      100/full  ap          10/100BaseTx
  11  manufacturing   up     up      auto      100/full  ap          10/100BaseTx
  12  manufacturing   up     up      auto      100/full  ap          10/100BaseTx
  13  manufacturing   up     up      auto      100/full  ap          10/100BaseTx
  14  rsrch_dev       up     up      auto      100/full  ap          10/100BaseTx
  15  rsrch_dev       up     up      auto      100/full  ap          10/100BaseTx
  16  rsrch_dev       up     up      auto      100/full  ap          10/100BaseTx
  17  rsrch_dev       up     up      auto      100/full  wired auth  10/100BaseTx
  18  rsrch_dev       up     up      auto      100/full  wired auth  10/100BaseTx
  19  mobility        up     up      auto      100/full  network     10/100BaseTx
  20  mobility        up     up      auto      100/full  network     10/100BaseTx
  21  backbone        up    down     auto                network
  22  backbone        up    down     auto                network
```

5 Configure ports 21 and 22 as a load-sharing port group to provide a redundant link to the backbone, and verify the configuration change. Type the following commands:

```
23x0# set port-group name backbonelink port 21,22 mode on
success: change accepted.
```

```
23x0# show port-group
Port group: backbonelink is up
        Ports:  22, 21
```

6 Add port 1 to the *default* VLAN (VLAN 1), configure a VLAN named *roaming* on ports 19 and 20, and verify the configuration changes. Type the following commands:

```
23x0# set vlan default port 1
success: change accepted.

23x0# set vlan 2 name roaming port 19-20
success: change accepted.

23x0# show vlan config
                  Admin  VLAN  Tunl                          Port
VLAN Name             Status State Affin Port              Tag
State
---- ---------------- ------ ----- ----- ---------------- -----
-----
   1 default          Up     Up        5
                                       1                 none Up
   2 roaming          Up     Up        5
                                       19                none Up
                                       20                none Up
```

7 Save the configuration. Type the following command:

```
23x0# save config
success: configuration saved.
```

Configuring and Managing IP Interfaces and Services

MTU Support 107
Configuring and Managing IP Interfaces 108
Configuring the System IP Address 114
Configuring and Managing IP Routes 117
Managing the Management Services 122
Configuring and Managing DNS 128
Configuring and Managing Aliases 133
Configuring and Managing Time Parameters 136
Managing the ARP Table 147
Pinging Another Device 150
Logging In to a Remote Device 151
Tracing a Route 152
IP Interfaces and Services Configuration Scenario 152

MTU Support

WLAN 2300 System Software (WSS Software) supports standard maximum transmission units (MTUs) of 1514 bytes for standard Ethernet packets and 1518 bytes for Ethernet packets with an 802.1Q tag. WSS Software does not support changing of the MTU through software configuration, and WSS Software does not do path MTU discovery.

Communication between WSSes is supported over any path MTU, and the Mobility Domain itself can run over the minimum IP path MTU. However, tunnels between two WSS switches require a path MTU of at least 1448 bytes.

This minimum MTU path is required because Nortel devices use IP tunnels to transport user traffic between WSS switches and to transport user traffic and control traffic between switches and AP access ports. Encapsulation of the packets for tunneling adds an additional 44 bytes to the packet headers, so WSS Software does fragment and reassemble the packets if necessary to fit within the supported MTUs. However, WSS Software does not support defragmentation except at the receiving end of an IP tunnel, and only to reassemble fragments created by another Nortel device for tunneling.

If the path MTU between Nortel devices is less than 1448 bytes, a device in the path might further fragment or drop a tunneled packet. If the packet is further fragmented, the receiving WSS will not be able to reassemble the fragments, and the packet is dropped.

Configuring and Managing IP Interfaces

Many features, including the following, require an IP interface on the WSS switch:

- Management access through Telnet
- Access by WLAN Management Software
- Exchanging information and user data with other WSS switches in a Mobility Domain

IP interfaces are associated with VLANs. At least one VLAN on an WSS switch must have an IP interface to provide management access. Optionally, the other VLANs configured on the switch also can each have an IP interface. Each IP interface must belong to a unique, non-overlapping IP subnet.

Adding an IP Interface

You can add an IP interface to a VLAN by statically configuring an IP address or by enabling the Dynamic Host Configuration Protocol (DHCP) client on the VLAN.

Statically Configuring an IP Interface

To add an IP interface to a VLAN, use the following command:

set interface *vlan-id* **ip** {*ip-addr mask* | *ip-addr*/*mask-length*}

Enabling the DHCP Client

The WSS Software DHCP client enables a WSS to obtain its IP configuration from a DHCP server. A switch can use the DHCP client to obtain the following configuration information:

- IP address
- Default gateway
- DNS domain name
- DNS server IP address

The DHCP client is implemented according to "RFC 2131: Dynamic Host Configuration Protocol" and "RFC 2132: DHCP Options and BOOTP Vendor Extensions". The client supports the following options:

- (12) Host Name (the WSS system name)
- (55) Parameter request list, consisting of (1) Subnet Mask, (3) Router, (15) Domain Name, and (6) Domain Name Server
- (60) Vendor Class Identifier, set to NORTEL *x.x.x*, where *x.x.x* is the WSS Software version

The DHCP client is enabled by default on an unconfigured WSS-2350 when the factory reset switch is pressed and held during power on. The DHCP client is disabled by default on all other switch models, and is disabled on an WSS-2350 if the switch is already configured or the factory reset switch is not pressed and held during power on.

You can enable the DHCP client on one VLAN only.

WSS Software also has a configurable DHCP server. (See "DHCP Server" on page 607.) You can configure a DHCP client and DHCP server on the same VLAN, but only the client or the server can be enabled. The DHCP client and DHCP server cannot both be enabled on the same VLAN at the same time.

How WSS Software Resolves Conflicts with Statically Configured IP Parameters

WSS Software compares the IP parameter values already configured on the switch with the values received from the DHCP server, and resolves any conflicts as follows:

- IP address—If the VLAN also has a statically configured IP address, WSS Software uses an address from the DHCP server instead of the statically configured address.

  WSS Software sends an ARP for the IP address offered by the DHCP server to verify that the address is not already in use.

  - If the address is not in use, WSS Software configures the VLAN that has the DHCP client enabled with the IP address received from the DHCP server. WSS Software then configures the other values as follows:

- Default gateway—WSS Software adds a default route for the gateway, with a metric of 10.
- DNS domain name and DNS server IP address—If the default domain name and DNS server IP address are already configured on the switch, and DNS is enabled, the configured values are used. Otherwise, the values received from the DHCP server are used.

- If the address offered by the DHCP server is already in use, WSS Software sends a DHCP Decline message to the server and generates a log message.
- If the address is in a subnet that is already configured on another VLAN on the switch, WSS Software sends a DHCP Decline message to the server and generates a log message.

If the switch is powered down or restarted, WSS Software does not retain the values received from the DHCP server. However, if the IP interface goes down but WSS Software is still running, WSS Software attempts to reuse the address when the interface comes back up.

Configuring the DHCP Client

To configure the DHCP client on a VLAN, use the following command:

set interface *vlan-id* **ip dhcp-client {enable | disable}**

The *vlan-id* can be the VLAN name or number.

The following command enables the DHCP client on VLAN *corpvlan*:

```
23x0# set interface corpvlan ip dhcp-client enable
success: change accepted.
```

You can configure the DHCP client on more than one VLAN, but the client can be active on only one VLAN.

To remove all IP information from a VLAN, including the DHCP client and user-configured DHCP server, use the following command:

clear interface *vlan-id* **ip**



Note. This command clears all IP configuration information from the interface.

The IP interface table flags the address assigned by a DHCP server with an asterisk (*). In the following example, VLAN *corpvlan* received IP address 10.3.1.110 from a DHCP server.

```
23x0# show interface
* = From DHCP
VLAN Name            Address         Mask            Enabled State RIB
---- --------------- --------------- --------------- ------- ----- --------
   4 corpvlan        *10.3.1.110     255.255.255.0   YES     Up    ipv4
```

Displaying DHCP Client Information

To display DHCP client information, type the following command:

```
23x0# show dhcp-client
 Interface:             corpvlan(4)
 Configuration Status: Enabled
 DHCP State:            IF_UP
 Lease Allocation:      65535 seconds
 Lease Remaining:       65532 seconds
 IP Address:            10.3.1.110
 Subnet Mask:           255.255.255.0
 Default Gateway:       10.3.1.1
 DHCP Server:           10.3.1.4
 DNS Servers:           10.3.1.29
 DNS Domain Name:       mycorp.com
```

Disabling or Reenabling an IP Interface

IP interfaces are enabled by default. To administratively disable or reenable an IP interface, use the following command:

set interface *vlan-id* **status {up | down}**

Removing an IP Interface

To remove an IP interface, use the following command:

clear interface *vlan-id* **ip**



Caution! If you remove the IP interface that is being used as the system IP address, features that require the system IP address will not work correctly.

Displaying IP Interface Information

To display IP interface information, use the following command:

show interface [*vlan-id*]

Configuring the System IP Address

You can designate one of the IP addresses configured on an WSS switch to be the system IP address of the switch. The system IP address determines the interface or source IP address WSS Software uses for system tasks, including the following:

- Mobility Domain operations
- Topology reporting for dual-homed AP access ports
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Designating the System IP Address

To designate the system IP address, use the following command:

set system ip-address *ip-addr*

Displaying the System IP Address

To display the system IP address, use the following command.

show system

Clearing the System IP Address



Caution! Clearing the system IP address disrupts the features that use the address.

To clear the system IP address, use the following command:

clear system ip-address

Configuring and Managing IP Routes

The IP route table contains routes that WSS Software uses for determining the interfaces for an WSS switch's external communications. When you add an IP interface to a VLAN that is up, WSS Software automatically adds corresponding entries to the IP route table.

For destination routes that are not directly attached, you can add static routes. A static route specifies the destination and the gateway router through which to forward traffic.You can add the following types of static routes:

- Explicit route—Forwarding path for traffic to a specific destination
- Default route—Forwarding path for traffic to a destination without an explicit route in the route table

A destination can be a subnet or network. If two static routes specify a destination, the more specific route is always chosen (longest prefix match). For example, if you have a static route with a destination of 10.10.1.0/24, and another static route with a destination of 10.10.0.0/16, the first static route is chosen to reach 10.10.1.15, because it has the longer prefix match.

If the IP route table contains an explicit route for a given destination, WSS Software uses the route. Otherwise, WSS Software uses a default route. For example, if the route table does not have a route to host 192.168.1.10, the WSS switch uses the default route to forward a packet addressed to that host. Nortel recommends that you configure at least one default route.

You can configure a maximum of four routes per destination. This includes default routes, which have destination 0.0.0.0/0. Each route to a given destination must have a unique gateway address. When the route table contains multiple default routes or multiple explicit routes to the same destination, WSS Software uses the route with the lowest metric (cost for using the route). If two or more routes to the same destination have the lowest cost, WSS Software selects the first route in the route table.

WSS Software can use a route only if the route is resolved by a direct route on one of the WSS switch's VLANs.



Note. Before you add a static route, use the **show interface** command to verify that the switch has an IP interface in the same subnet as the route's gateway router. WSS Software requires the routes for the interface to resolve the static route. If the switch does not have an interface in the gateway's subnet, the static route cannot be resolved and the VLAN:Interface field of the **show ip route** command output shows that the static route is down.

Displaying IP Routes

To display IP routes, use the following command:

show ip route [*destination*]

The *destination* parameter specifies a destination IP address.

To display the IP route table, type the following command:

23x0# **show ip route**

```
Router table for IPv4
Destination/Mask   Proto   Metric NH-Type Gateway          VLAN:Interface
_________________ _______ ______ _______ _______________ _______________

        0.0.0.0/ 0 Static       1 Router  10.0.1.17       vlan:1:ip
        0.0.0.0/ 0 Static       2 Router  10.0.2.17       vlan:2:ip
       10.0.1.1/24 IP           0 Direct                  vlan:1:ip
     10.0.1.1/32 IP         0 Local                   vlan:1:ip:10.0.1.1/24
   10.0.1.255/32 IP         0 Local                   vlan:1:ip:10.0.1.1/24
      10.0.2.1/24 IP           0 Direct                  vlan:2:ip
    10.0.2.1/32 IP         0 Local                   vlan:2:ip:10.0.1.1/24
   10.0.2.255/32 IP         0 Local                   vlan:2:ip:10.0.1.1/24
     224.0.0.0/ 4 IP           0 Local                   MULTICAST
```

This example shows dynamic routes added by WSS Software for two VLAN interfaces, 10.0.1.1/24 on VLAN 1 and 10.0.2.1/24 on VLAN 2.

This example also shows two static routes, which have a next-hop type (NH-Type) value of Router. Static routes have a gateway router, listed in the Gateway field. The 0.0.0.0 destination represents a default route. Here, gateway router 10.0.1.17 is reachable through the subnet on VLAN 1. Route 10.0.1.1/24 resolves the static route that uses the gateway router. Gateway router 10.0.2.17 is reachable through the subnet on VLAN 2 and route 10.0.2.1/24 resolves the static route to that gateway.

WSS Software adds routes with next-hop types Direct and Local when you add an IP interface to a VLAN, when the VLAN is up. Direct routes are for the locally attached subnets that the switch's IP addresses are in. Local routes are for destination interfaces configured on the WSS switch itself.

WSS Software automatically adds the 224.0.0.0 route to support the IGMP snooping feature.

If a VLAN is administratively disabled or all of the links in the VLAN go down or are disabled, WSS Software removes the VLAN's routes from the route table. If the direct route required by a static route goes down, WSS Software changes the static route state to Down. If the route table contains other static routes to the same destination, WSS Software selects the resolved route that has the lowest cost. In the following example, the default route to 10.0.1.17 is down, so WSS Software selects the default route to 10.0.2.17.

23x0# **show ip route**

```
Router table for IPv4
Destination/Mask   Proto   Metric NH-Type Gateway          VLAN:Interface
_________________ _______ ______ _______ _______________ _______________

        0.0.0.0/ 0 Static       1 Router  10.0.1.17       Down
        0.0.0.0/ 0 Static       2 Router  10.0.2.17       vlan:2:ip
       10.0.2.1/24 IP           0 Direct                  vlan:2:ip
     10.0.2.1/32 IP         0 Direct                  vlan:2:ip:10.0.1.1/24
    10.0.2.255/32 IP         0 Direct                  vlan:2:ip:10.0.1.1/24
```

```
      224.0.0.0/ 4 IP           0 Local                    MULTICAST
```

(For more information about the fields in the output, see the *Nortel WLAN Security Switch 2300 Software Command Reference*.)

Adding a Static Route

To add a static route, use the following command:

set ip route {**default** | *ip-addr mask* | *ip-addr*/*mask-length*} *gateway metric*

The metric (cost) can be any number between 0 and 2,147,483,647. Lower-cost routes are preferred over higher-cost routes. When you add multiple routes to the same destination, WSS Software groups the routes together and orders them from lowest cost at the top of the group to highest cost at the bottom of the group. If you add a new route that has the same destination and cost as a route already in the table, WSS Software places the new route at the top of the group of routes with the same cost.

To add a default route that uses gateway 10.5.4.1 and has a cost of 1, type the following command:

```
23x0# set ip route default 10.5.4.1 1
success: change accepted.
```

To add two default routes and configure WSS Software to always use the route through 10.2.4.69 when the WSS interface to that gateway router is up, type the following commands:

```
23x0# set ip route default 10.2.4.69 1
success: change accepted.
```

```
23x0# set ip route default 10.2.4.17 2
success: change accepted.
```

To add an explicit route from an WSS switch to any host on the 192.168.4.*x* subnet through the local router 10.5.4.2, and give the route a cost of 1, type the following command:

```
23x0# set ip route 192.168.4.0 255.255.255.0 10.5.4.2 1
success: change accepted.
```

Removing a Static Route

To remove a static route, use the following command:

clear ip route {**default** | *ip-addr mask* | *ip-addr/mask-length*} *gateway*

Note. After you remove a route, traffic that uses the route can no longer reach its destination. For example, if you are managing the WSS switch with a Telnet session and the session needs the static route, removing the route also removes the Telnet connection to the switch.

The following command removes the route to 192.168.4.69/24 that uses gateway router 10.2.4.1:

```
23x0# clear ip route 192.168.4.69/24 10.2.4.1
success: change accepted.
```

The following command removes the default route that uses gateway router 10.5.5.5:

```
23x0# clear ip route default 10.5.5.5
success: change accepted.
```

Managing the Management Services

WSS Software provides the following services for managing an WSS switch over the network:

Secure Shell (SSH)	SSH provides a secure connection to the CLI through TCP port 22.
Telnet	Telnet provides a nonsecure connection to the CLI through TCP port 23.
HTTPS	HTTPS provides a secure connection to the Web management application through TCP port 443.

SSH is enabled by default. Telnet and HTTPS are disabled by default.

A WSS can have up to eight Telnet or SSH sessions, in any combination, and one Console session.

Managing SSH

WSS Software supports Secure Shell (SSH) Version 2. SSH provides secure management access to the CLI over the network. SSH requires a valid username and password for access to the switch. When a user enters a valid username and password, SSH establishes a management session and encrypts the session data.

Login Timeouts

When you access the SSH server on a WSS, WSS Software allows you 10 seconds to press Enter for the username prompt. After the username prompt is displayed, WSS Software allows 30 seconds to enter a valid username and password to complete the login. If you do not press Enter or complete the login before the timer expires, WSS Software ends the session. These timers are not configurable.

Session Timeouts

Each SSH session is governed by two timeouts:

- Idle timeout—controls how long an open SSH session can remain idle before WSS Software closes the session. The default idle timeout is 30 minutes. You can set the idle timeout to a value from 0 (disabled) to 2,147,483,647 minutes.
- Absolute timeout—controls how long an SSH session can remain open, regardless of how active the session is. The absolute timeout is disabled by default. Nortel recommends using the idle timeout to close unused sessions. However, if the idle timeout is disabled, WSS Software changes the default absolute timeout from 0 (disabled) to 60 minutes to prevent an abandoned session from remaining open indefinitely. You can set the absolute timeout to a value from 0 (disabled) to 2,147,483,647 minutes.



Note. To ensure that all CLI management sessions are encrypted, after you configure SSH, disable Telnet.

Enabling SSH

SSH is enabled by default. However, to use SSH, you must generate an SSH authentication key, using the following command:

crypto generate key ssh {1024 | 2048}

To disable or reenable SSH, use the following command:

set ip ssh server {enable | disable}

You must generate an SSH authentication key before you can enable SSH. You need to generate the key only once. The key must be at least 1024 bytes long. The WSS stores the key in nonvolatile storage where the key remains even after software reboots.

To generate a 1024-byte SSH authentication key, type the following command:

```
23x0# crypto generate key ssh 1024
key pair generated
```

You can verify the key using the following command:

show crypto key ssh

For example:

```
23x0# show crypto key ssh
ec:6f:56:7f:d1:fd:c0:28:93:ae:a4:f9:7c:f5:13:04
```

This command displays the checksum (also called a *fingerprint*) of the public key. When you initially connect to the WSS with an SSH client, you can compare the SSH key checksum displayed by the WSS switch with the one displayed by the client to verify that you really are connected to the WSS and not another device. Generally, SSH clients remember the encryption key after the first connection, so you need to check the key only once.

Adding an SSH User

To log in with SSH, a user must supply a valid username and password. To add a username and password to the local database, use the following command:

set user *username* **password** *password*

Optionally, you also can configure WSS Software either to locally authenticate the user or to use a RADIUS server to authenticate the user. Use the following command:

set authentication admin {*user-wildcard*} *method1* [*method2*] [*method3*] [*method4*]

To add administrative user *WSSadmin* with password *letmein*, and use RADIUS server group *sg1* to authenticate the user, type the following commands:

```
23x0# set user WSSadmin password letmein
success: User WSSadmin created

23x0# set authentication admin WSSadmin sg1
success: change accepted
```

(For more information, see "Adding and Clearing Local Users for Administrative Access" on page 63.)

Changing the SSH Service Port Number

To change the SSH port the WSS listens on for SSH connections, use the following command:

set ip ssh port *port-num*



Caution! If you change the SSH port number from an SSH session, WSS Software immediately ends the session. To open a new management session, you must configure the SSH client to use the new SSH port number.

Changing SSH Timeouts

To change the SSH timeout values, use the following commands:

set ip ssh idle-timeout *minutes*

set ip ssh absolute-timeout *minutes*

To change the absolute timeout value to 30 minutes, type the following command:

```
23x0# set ip ssh absolute-timeout 30
success: absolute timeout set to 30 minutes
```

Managing SSH Server Sessions

Use the following commands to manage SSH server sessions:

show sessions admin

clear sessions admin ssh [*session-id*]

These commands display and clear SSH server sessions.



Note. If you type the **clear sessions admin ssh** command from within an SSH session, the session ends as soon as you press Enter.

To display the SSH server sessions on a WSS, type the following command:

```
23x0# show sessions admin
Tty          Username              Time (s)     Type
-------      --------------------  --------     ----
tty0                               3644         Console
tty2         tech                  6            Telnet
tty3         sshadmin              381          SSH

3 admin sessions
```

To clear all SSH server sessions, type the following command:

```
23x0# clear sessions admin ssh
Thiswillterminatemanagersessions,doyouwishtocontinue?(y|n)[n]y
Cleared ssh session on tty3
```

(To manage Telnet client sessions, see "Logging In to a Remote Device" on page 151.)

Managing Telnet

Telnet requires a valid username and password for access to the switch.

Telnet Login Timers

After the username prompt is displayed, WSS Software allows 30 seconds to enter a valid username and password to complete the login. If you do not press Enter or complete the login before the timer expires, WSS Software ends the session. This timer is not configurable.

Enabling Telnet

Telnet is disabled by default. To enable Telnet, use the following command:

set ip telnet server {**enable** | **disable**}

Adding a Telnet User

To log in with Telnet, a user must supply a valid username and password. To add a username and password to the local database, use the following command:

set user *username* **password** *password*

Optionally, you also can configure WSS Software either to locally authenticate the user or to use a RADIUS server to authenticate the user. Use the following command:

set authentication admin {*user-wildcard*} *method1* [*method2*] [*method3*] [*method4*]

You can use the same username and password for SSH or create a new one. For a CLI example, see "Adding an SSH User" on page 124.

Displaying Telnet Status

To display the status of the Telnet server, use the following command:

show ip telnet

To display the Telnet server status and the TCP port number on which a WSS switch listens for Telnet traffic, type the following command:

```
WSS-20> show ip telnet

Server Status                  Port
---------------------------------
Enabled                         23
```

Changing the Telnet Service Port Number

To change the TCP port the WSS listens on for Telnet connections, use the following command:

set ip telnet *port-num*



Caution! If you change the Telnet port number from a Telnet session, WSS Software immediately ends the session. To open a new management session, you must Telnet to the switch with the new Telnet port number.

Resetting the Telnet Service Port Number to Its Default

To reset the Telnet management service to its default TCP port, use the following command:

clear ip telnet

Managing Telnet Server Sessions

Use the following commands to manage Telnet server sessions:

show sessions admin

clear sessions admin telnet [*session-id*]

These commands display and clear management sessions from a remote client to the WSS's Telnet server.



Note. If you type the **clear sessions admin telnet** command from within a Telnet session, the session ends as soon as you press Enter.

To display the Telnet server sessions on an WSS switch, type the following command:

```
23x0# show sessions admin
Tty          Username              Time (s)     Type
-------      --------------------  --------     ----
tty0                               3644         Console
tty2         tech                  6            Telnet
tty3         sshadmin              381          SSH

3 admin sessions
```

To clear all Telnet server sessions, type the following command:

```
23x0# clear sessions telnet
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
Cleared telnet session on tty2
```

(To manage Telnet client sessions, see "Logging In to a Remote Device" on page 151.)

Managing HTTPS

Enabling HTTPS

HTTPS is disabled by default. To enable HTTPS, use the following command:

set ip https server {enable | disable}



Caution! If you disable the HTTPS server, Web View access to the switch is also disabled.

Displaying HTTPS Information

To display HTTPS service information, use the following command:

show ip https

To display information for an WSS switch's HTTPS server, type the following command:

```
WSS-20> show ip https
HTTPS is enabled
HTTPS is set to use port 443

Last 10 Connections:
 IP Address     Last Connected          Time Ago (s)
------------    ---------------------- ------------
10.10.10.56     2003/05/09 15:51:26 pst          349
```

The command lists the TCP port number on which the switch listens for HTTPS connections. The command also lists the last 10 devices to establish HTTPS connections with the switch and when the connections were established.

If a browser connects to an WSS switch from behind a proxy, then only the proxy IP address is shown. If multiple browsers connect using the same proxy, the proxy address appears only once in the output.

Configuring and Managing DNS

You can configure an WSS switch to use a Domain Name Service (DNS) server to resolve hostnames into their IP addresses. This capability is useful in cases where you specify a hostname instead of an IP address in a command.

For example, as an alternative to the command **ping 192.168.9.1**, you can enter the command **ping chris.example.com**. When you enter **ping chris.example.com**, the WSS switch's DNS client queries a DNS server for the IP address that corresponds to the hostname *chris.example.com*, then sends the ping request to that IP address.

The WSS switch's DNS client is disabled by default. To configure DNS:

- Enable the DNS client.
- Specify the IP addresses of the DNS servers.
- Configure a default domain name for DNS queries.

Enabling or Disabling the DNS Client

The DNS client is disabled by default. To enable or disable the DNS client, use the following command:

set ip dns {enable | disable}

Configuring DNS Servers

You can configure an WSS switch to use one primary DNS server and up to five secondary DNS servers to resolve DNS queries.

The WSS switch always sends a request to the primary DNS server first. The WSS switch sends a request to a secondary DNS server only if the primary DNS server does not respond.

Adding a DNS Server

To add a DNS server, use the following command:

set ip dns server *ip-addr* **{primary | secondary}**

Removing a DNS Server

To remove a DNS server, use the following command:

clear ip dns server *ip-addr*

Configuring a Default Domain Name

You can configure a single default domain name for DNS queries. The WSS appends the default domain name to hostnames you enter in commands. For example, you can configure the WSS to automatically append the domain name *example.com* to any hostname that does not have a domain name. In this case, you can enter **ping chris** instead of **ping chris.example.com**, and the WSS automatically requests the DNS server to send the IP address for *chris.example.com*.

To override the default domain name when entering a hostname in a CLI command, enter a period at the end of the hostname. For example, if the default domain name is *example.com*, enter **chris.** if the hostname is *chris* and not *chris.example.com*.

Aliases take precedence over DNS. When you enter a hostname, WSS Software checks for an alias with that name first, before using DNS to resolve the name. (For information about aliases, see "Configuring and Managing Aliases" on page 133.)

Adding the Default Domain Name

To add the default domain name, use the following command:

set ip dns domain *name*

Specify a domain name of up to 64 alphanumeric characters.

Removing the Default Domain Name

To remove the default domain name, use the following command:

clear ip dns domain

Displaying DNS Server Information

To display DNS server information, use the following command:

show ip dns

The following example shows DNS server information on an WSS switch configured to use three DNS servers.

```
23x0# show ip dns
Domain Name: example.com
DNS Status: enabled
IP Address                Type
-----------------------------------
10.1.1.1                  PRIMARY
10.1.1.2                  SECONDARY
10.1.2.1                  SECONDARY
```

(For information about the fields in the output, see the *Nortel WLAN Security Switch 2300 Software Command Reference*.)

Configuring and Managing Aliases

An alias is a string that represents an IP address. You can use aliases as shortcuts in CLI commands. For example, you can configure alias *pubs1* for IP address 10.10.10.20, and enter **ping pubs1** as a shortcut for **ping 10.10.10.20**.

Aliases take precedence over DNS. When you enter a hostname, WSS Software checks for an alias with that name first, before using DNS to resolve the name.

Adding an Alias

To add an alias, use the following command:

set ip alias *name ip-addr*

Specify an alias of up to 32 alphanumeric characters.

To add an alias *HR1* for IP address 192.168.1.2, type the following command:

```
23x0# set ip alias HR1 192.168.1.2
success: change accepted.
```

After configuring the alias, you can use *HR1* in commands in place of the IP address. For example, to ping 192.168.1.2, you can type the command **ping HR1**.

Removing an Alias

To remove an alias, use the following command:

clear ip alias *name*

Displaying Aliases

To display aliases, use the following command:

show ip alias [*name*]

Here is an example:

```
23x0# show ip alias
Name                    IP Address
--------------------    --------------------
HR1                     192.168.1.2
payroll                 192.168.1.3
radius1                 192.168.7.2
```

Configuring and Managing Time Parameters

You can configure the system time and date statically or by using Network Time Protocol (NTP) servers. In each case, you can specify the offset from Coordinated Universal Time (UTC) by setting the time zone. You also can configure WSS Software to offset the time by an additional hour for daylight savings time or similar summertime period.

Note. Nortel recommends that you set the time and date parameters before you install certificates on the WSS switch. Generally, certificates are valid for one year beginning with the system time and date that are in effect when you generate the certificate request. If the switch's time and date are incorrect, the certificate might not be valid.

To statically set the time and date:

- Set the time zone (**set timezone** command)
- Set the summertime period (**set summertime** command)
- Set the time and date (**set timedate** command)

Note. Configure summertime *before* you set the time and date. Otherwise, summertime's adjustment of the time will make the time incorrect, if the date is within the summertime period.

To use NTP servers to set the time and date:

- Set the time zone (**set timezone** command)
- Set the summertime period (**set summertime** command)
- Configure NTP server information (**set ntp** commands)

Setting the Time Zone

The time zone parameter adjusts the system date, and optionally the time, by applying an offset to UTC.

To set the time zone, use the following command:

set timezone *zone-name* {-*hours* [*minutes*]}

The zone name can be up to 32 alphanumeric characters long, with no spaces. The *hours* parameter specifies the number of hours to add to or subtract from UTC. Use a minus sign (-) in front of the hour value to subtract the hours from UTC.

To set the time zone to *PST* (Pacific Standard Time), type the following command:

```
23x0# set timezone PST -8
Timezone is set to 'PST', offset from UTC is -8:0 hours.
```

Displaying the Time Zone

To display the time zone, use the following command:

show timezone

For example, to display the time zone, type the following command:

```
23x0# show timezone
Timezone set to 'PST', offset from UTC is -8 hours
```

Clearing the Time Zone

To clear the time zone, use the following command:

clear timezone

Configuring the Summertime Period

The summertime period offsets the system time +1 hour and returns it to standard time for daylight savings time or a similar summertime period that you set.



Note. Configure summertime *before* you set the time and date. Otherwise, summertime's adjustment of the time will make the time incorrect, if the date is within the summertime period.

To configure the summertime period, use the following command:

set summertime *summer-name* [**start** *week weekday month hour min* **end** *week weekday month hour min*]

The *summer-name* can be up to 32 alphanumeric characters long, with no spaces. The start and end dates and times are optional. If you do not specify a start and end time, WSS Software implements the time change starting at 2:00 a.m. on the first Sunday in April and ending at 2:00 a.m. on the last Sunday in October, according to the North American standard.

To set the summertime period to *PDT* (Pacific Daylight Time) and use the default start and end dates and times, type the following command:

```
23x0# set summertime PDT
success: change accepted.
```

Displaying the Summertime Period

To display the summertime period, use the following command:

show summertime

For example, to display the summertime period, type the following command:

```
23x0# show summertime
Summertime is enabled, and set to 'PDT'.
  Start  : Sun Apr 04 2004, 02:00:00
  End    : Sun Oct 31 2004, 02:00:00
  Offset : 60 minutes
  Recurring : yes, starting at 2:00 am of first Sunday of April
              and ending at 2:00 am on last Sunday of October.
```

(For information about the fields in the output, see the *Nortel WLAN Security Switch 2300 Software Command Reference*.)

Clearing the Summertime Period

To clear the summertime period, use the following command:

clear summertime

Statically Configuring the System Time and Date

To statically configure the system time and date, use the following command:

set timedate {**date** *mmm dd yyyy* [**time** *hh:mm:ss*]}

The day of week is automatically calculated from the day you set.

To set the date to February 29, 2004 and time to 23:58:

```
23x0# set timedate date feb 29 2004 time 23:58:00
Time now is:              Sun Feb 29 2004, 23:58:02 PST
```

The CLI makes the time change, then displays the current system time based on the change. (The time displayed might be slightly later than the time you enter due to the interval between when you press Enter and when the CLI reads and displays the new time and date.)

Displaying the Time and Date

To display the time and date, use the following command:

show timedate

```
23x0# show timedate
Sun Feb 29 2004, 23:58:02 PST
```

Configuring and Managing NTP

The Network Time Protocol (NTP) allows a networking device to synchronize its system time and date with the time and date on an NTP server. When used on multiple devices, NTP ensures that the time and date are consistent among those devices.

The NTP implementation in WSS Software is based on RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

You can configure a WSS to consult up to three NTP servers. The switch compares the results from the servers and selects the best response. (For information, see RFC 1305.)

After you enable the NTP client and configure NTP servers, WSS Software queries the NTP servers for an update every 64 seconds and waits 15 seconds for a reply. If the switch does not receive a reply to an NTP query within 15 seconds, the switch tries again up to 16 times. You can change the update interval but not the timeout or number of retries.

WSS Software adjusts the NTP reply according to the following time parameters configured on the WSS switch:

- Offset from UTC (configured with the **timezone** command; see "Setting the Time Zone" on page 137)
- Daylight savings time (configured with the **set summertime** command; see "Configuring the Summertime Period" on page 138)

The NTP client is disabled by default.



Note. If NTP is configured on a system whose current time differs from the NTP server time by more than 10 minutes, convergence of the WSS time may take many NTP update intervals. Nortel recommends that you set the time manually to the NTP server time before enabling NTP to avoid a significant delay in convergence.

Adding an NTP Server

To add an NTP server to the list of NTP servers, use the following command:

set ntp server *ip-addr*

To configure a WSS to use NTP server 192.168.1.5, type the following command:

```
23x0# set ntp server 192.168.1.5
```

Removing an NTP Server

To remove an NTP server, use the following command:

clear ntp server {*ip-addr* | **all**}

If you use the **all** option, WSS Software clears all NTP servers configured on the switch.

Changing the NTP Update Interval

The default update interval is 64 seconds. To change the update interval, use the following command:

set ntp update-interval *seconds*

You can specify an interval from 16 through 1024 seconds.

For example, to change the NTP update interval to 128 seconds, type the following command:

```
23x0# set ntp update-interval 128
success: change accepted.
```

Resetting the Update Interval to the Default

To reset the update interval to the default value, use the following command:

clear ntp update-interval

Enabling the NTP Client

The NTP client is disabled by default. To enable the NTP client, use the following command:

set ntp {enable | disable}

Displaying NTP Information

To display NTP information, use the following command:

show ntp

Here is an example:

```
WSS-20> show ntp
NTP client: enabled
Current update-interval: 20(secs)
Current time: Sun Feb 29 2004, 23:58:12
Timezone is set to 'PST', offset from UTC is -8:0 hours.
Summertime is enabled.
Last NTP update: Sun Feb 29 2004, 23:58:00
NTP Server          Peer state          Local State
-------------------------------------------------
192.168.1.5         SYSPEER             SYNCED
```

The Timezone and Summertime fields are displayed only if you change the timezone or enable summertime.

(For more information about the fields in the output, see the *Nortel WLAN Security Switch 2300 Software Command Reference*.)

Managing the ARP Table

The Address Resolution Protocol (ARP) table maps IP addresses to MAC addresses. An ARP entry enters the table in one of the following ways:

- Added automatically by the WSS. A switch adds an entry for its own MAC address and adds entries for addresses learned from traffic received by the WSS. When the WSS receives an IP packet, the switch adds the packet's source MAC address and source IP address to the ARP table.
- Added by the system administrator. You can add dynamic, static, and permanent entries to the ARP table.

ARP is enabled by default on a WSS and cannot be disabled.

Displaying ARP Table Entries

To display ARP table entries, use the following command:

show arp [*ip-addr*]

Here is an example:

```
23x0# show arp
ARP aging time: 1200 seconds

Host                           HW Address        VLAN  Type    State
------------------------------ ----------------- ----- ------- --------
10.5.4.51                      00:0b:0e:02:76:f5     1 DYNAMIC RESOLVED
10.5.4.53                      00:0b:0e:02:76:f7     1 LOCAL   RESOLVED
```

This example shows two entries. The local entry (with LOCAL in the Type field) is for the WSS switch itself. The MAC address of the local entry is the switch's MAC address. The ARP table contains one local entry for each VLAN configured on the switch. The dynamic entry is learned from traffic received by the switch. The ARP table can also contain static and permanent entries, which are added by an administrator. The State field indicates whether an entry is resolved (RESOLVED) or whether WSS Software has sent an ARP request for the entry and is waiting for the reply (RESOLVING).

Adding an ARP Entry

WSS Software automatically adds a local entry for a WSS and dynamic entries for addresses learned from traffic received by the switch. You can add the following types of entries:

- Dynamic—Ages out based on the aging timeout.
- Static—Does not age out but is removed by a software reboot.
- Permanent—Does not age out and remains in the ARP table following a software reboot.

To add an ARP entry, use the following command:

set arp {permanent | static | dynamic} *ip-addr mac-addr*

To add a static ARP entry that maps IP address 10.10.10.1 to MAC address 00:bb:cc:dd:ee:ff, type the following command:

```
23x0# set arp static 10.10.10.1 00:bb:cc:dd:ee:ff
success: added arp 10.10.10.1 at 00:bb:cc:dd:ee:ff on VLAN 1
```

Changing the Aging Timeout

The aging timeout specifies how long a dynamic entry can remain unused before the software removes the entry from the ARP table. The default aging timeout is 1200 seconds (20 minutes). The aging timeout does not affect the local entry, static entries, or permanent entries.

To change the aging timeout, use the following command:

set arp agingtime *seconds*

You can specify from 0 to 1,000,000 seconds. To disable aging, specify 0.

For example, to disable aging of dynamic ARP entries, type the following command:

```
23x0# set arp agingtime 0
success: set arp aging time to 0 seconds
```



Note. To reset the ARP aging timeout to its default value, use the **set arp agingtime 1200** command.

Pinging Another Device

To verify that another device in the network can receive IP packets sent by the WSS switch, use the following command:

ping *host* [**count** *num-packets*] [**dnf**] [**flood**] [**interval** *time*] [**size** *size*] [**source-ip** *ip-addr* | *vlan-name*]

To ping a device that has IP address 10.1.1.1, type the following command:

```
23x0# ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1) from 10.9.4.34 : 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.769 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.628 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.676 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.619 ms
64 bytes from 10.1.1.1: icmp_seq=5 ttl=255 time=0.608 ms
--- 10.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0 errors, 0% packet loss
```

In this example, the ping is successful, indicating that the WSS has IP connectivity with the other device.

(For information about the command options, see the *Nortel WLAN Security Switch 2300 Software Command Reference*.)

Logging In to a Remote Device

From within an WSS Software console session or Telnet session, you can use the Telnet client to establish a Telnet client session from a WSS switch's CLI to another device. To establish a Telnet client session with another device, use the following command:

telnet {*ip-addr* | *hostname*} [**port** *port-num*]

To establish a Telnet session from WSS 2370 to 10.10.10.90, type the following command:

```
23x0# telnet 10.10.10.90
Session 0 pty tty2.d Trying 10.10.10.90...
Connected to 10.10.10.90
Disconnect character is '^t'

Copyright (c) 2002, 2003
        Nortel , Inc.

Username:
```

When you press Ctrl+t or type **exit** to end the client session, the management session returns to the local WSS prompt:.

```
WSS-2370-remote> Session 0 pty tty2.d terminated tt name tty2.d
WSS-2370#
```

Use the following commands to manage Telnet client sessions:

show sessions telnet client

clear sessions telnet client [*session-id*]

These commands display and clear Telnet sessions from a WSS's Telnet client to another device.

To display the Telnet client sessions on a WSS, type the following command:

```
23x0# show sessions telnet client
Session   Server Address    Server Port    Client Port
-------   --------------    -------------  -----------
0          192.168.1.81     23             48000
1           10.10.1.22      23             48001
```

To clear Telnet client session 0, type the following command:

```
23x0# clear sessions telnet client 0
```

You also can clear a Telnet client session by typing **exit** from within the client session.

Tracing a Route

You can trace the router hops necessary to reach an IP host.

The traceroute facility uses the TTL (Time to Live) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a UDP datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an ICMP *Time Exceeded* message to the sender.

The traceroute facility determines the address of the first hop by examining the source address field of the ICMP time-exceeded message.

To identify the next hop, traceroute again sends a UDP packet, but this time with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the *Time Exceeded* message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To determine when a datagram has reached its destination, traceroute sets the UDP destination port in the datagram to a very large value, one that the destination host is unlikely to be using. In addition, when a host receives a datagram with an unrecognized port number, it sends an ICMP *Port Unreachable* error to the source. This message indicates to the traceroute facility that it has reached the destination.

To trace a route to a destination subnet, use the following command:

traceroute *host* **[dnf] [no-dns] [port** *port-num***] [queries** *num***] [size** *size***] [ttl** *hops***] [wait** *ms***]**

To trace the route to host *server1*, type the following command:

```
23x0# traceroute server1
traceroute to server1.example.com (192.168.22.7), 30 hops max, 38 byte packets
1 engineering-1.example.com (192.168.192.206) 2 ms 1 ms 1 ms
2 engineering-2.example.com (192.168.196.204) 2 ms 3 ms 2 ms
3 gateway_a.example.com (192.168.1.201) 6 ms 3 ms 3 ms
4 server1.example.com (192.168.22.7) 3 ms * 2 ms
```

In this example, *server1* is four hops away. The hops are listed in order, beginning with the hop that is closest to the WSS and ending with the route's destination. (For information about the command options, see the *Nortel WLAN Security Switch 2300 Software Command Reference.*)

IP Interfaces and Services Configuration Scenario

This scenario configures IP interfaces, assigns one of the interfaces to be the system IP address, and configures a default route, DNS parameters, and time and date parameters.

1 Configure IP interfaces on the *WSS_mgmt* and *roaming* VLANs, and verify the configuration changes. Type the following commands:

```
23x0# set interface WSS_mgmt ip 10.10.10.10/24
success: change accepted.
```

```
23x0# set interface roaming ip 10.20.10.10/24
success: change accepted.
```

```
23x0# show interface
* = From DHCP
VLAN Name            Address         Mask            Enabled State RIB
---- --------------- --------------- --------------- ------- ----- --------
   1 default         10.10.10.10     255.255.255.0   YES     Up    ipv4
   2 roaming         10.20.10.10     255.255.255.0   YES     Up    ipv4
```

2 Configure the IP interface on the *roaming* VLAN to be the system IP address and verify the configuration change. Type the following commands:

```
23x0# set system ip-address 10.20.10.10
success: change accepted.
23x0# show system
================================================================================
 Product Name:       WSS-20
 System Name:        WSS-20
 System Countrycode: US
 System Location:
 System Contact:
 System IP:          10.02.10.10
 System MAC:         00:0B:0E:00:04:0C
 License:            unlimited
================================================================================
 Boot Time:          2000-03-18 22:59:19
 Uptime:                 0 days 01:12:02
================================================================================
 Fan status:  fan1 OK fan2 OK fan3 OK
 Temperature: temp1 ok  temp2 ok  temp3 ok
 PSU Status:  Lower Power Supply DC ok AC ok  Upper Power Supply missing
 Memory:      156.08/496.04 (31%)
 Total Power Over Ethernet : 105.6
================================================================================
```

3 Configure a default route through a gateway router attached to the WSS switch and verify the configuration change. Type the following commands:

```
23x0# set ip route default 10.20.10.1 1
success: change accepted.
23x0# show ip route
Router table for IPv4
Destination/Mask   Proto   Metric NH-Type Gateway          VLAN:Interface
_________________ _______ ______ _______ _______________ _______________

       0.0.0.0/ 0 Static       1 Router  10.20.10.1
    10.10.10.10/24 IP          0 Direct                    vlan:1:ip
    10.10.10.10/32 IP          0 Local                   vlan:1:ip:10.10.10.10/24
    10.20.10.10/24 IP          0 Direct                    vlan:1:ip
    10.20.10.10/32 IP          0 Local                   vlan:1:ip:10.20.10.10/24
      224.0.0.0/ 4 IP          0 Local                     MULTICAST
```

4 Configure the DNS domain name and DNS server entries, enable the DNS service, and verify the configuration changes. Type the following commands:

```
23x0# set ip dns domain example.com
success: change accepted.

23x0# set ip dns server 10.10.10.69 PRIMARY
```

```
success: change accepted.
```

23x0# **set ip dns server 10.20.10.69 SECONDARY**

```
success: change accepted.
```

23x0# **set ip dns enable**

```
success: change accepted.
```

23x0# **show ip dns**

```
Domain Name: example.com
DNS Status: enabled
IP Address                Type
----------------------------------
10.10.10.69               PRIMARY
10.20.10.69               SECONDARY
```

5 Configure time zone, summertime, and NTP parameters and verify the configuration changes. Type the following commands:

23x0# **set timezone PST -8**

```
success: change accepted.
```

23x0# **show timezone**

```
Timezone is set to 'PST', offset from UTC is -8:0 hours.
```

23x0# **set summertime PDT**

```
success: change accepted.
```

23x0# **show summertime**

```
Summertime is enabled, and set to 'PDT'.
  Start  : Sun Apr 04 2004, 02:00:00
  End    : Sun Oct 31 2004, 02:00:00
  Offset : 60 minutes
  Recurring : yes, starting at 2:00 am of first Sunday of April
```

Configuring SNMP

Overview 155
Configuring SNMP 155
Displaying SNMP Information 167

WSS Software supports Simple Network Management Protocol (SNMP) versions 1, 2c, and 3.

Overview

The WSS Software SNMP engine (also called the SNMP *server* or *agent*) can run any combination of the following SNMP versions:

- SNMPv1—SNMPv1 is the simplest and least secure SNMP version. Community strings are used for authentication. Communications are in the clear (not encrypted). Notifications are traps, which are not acknowledged by the notification target (also called a *trap receiver*).
- SNMPv2c—SNMPv2 is similar to SNMPv1, but supports informs. An inform is a notification that is acknowledged by the notification target.
- SNMPv3—SNMPv3 adds authentication and encryption options. Instead of community strings, SNMPv3 supports user security model (USM) users, with individually configurable access levels, authentication options, and encryption options.

All SNMP versions are disabled by default.

Configuring SNMP

To configure SNMP, perform the following tasks:

- Set the switch's system IP address, if it is not already set. SNMP will not work without the system IP address. (See "Configuring the System IP Address" on page 114.)
- Optionally, set the system location and contact strings.
- Enable the SNMP version(s) you want to use. WSS Software can run one or more versions, in any combination.
- Configure community strings (for SNMPv1 or SNMPv2c) or USM users (for SNMPv3).
- Set the minimum level of security allowed for SNMP message exchanges.
- Configure a notification profile or modify the default one, to enable sending of notifications to notification targets. By default, notifications of all types are dropped (not sent).
- Configure notification targets.
- Enable the WSS Software SNMP engine.

Setting the System Location and Contact Strings

To set the location and contact strings for a switch, use the following commands:

set system location *string*

set system contact *string*

Each string can be up to 256 characters long, with no blank spaces.

The following commands set a WSS's location to *3rd_floor_closet* and set the contact to *sysadmin1*:

```
23x0# set system location 3rd_floor_closet
success: change accepted.

23x0# set system contact sysadmin1
success: change accepted.
```

Enabling SNMP Versions

To enable an SNMP protocol, use the following command:

set snmp protocol {v1 | v2c | usm | all} {enable | disable}

The **usm** option enables SNMPv3. The **all** option enables all three versions of SNMP.

The following command enables all SNMP versions:

```
23x023x0# set snmp protocol all enable
success: change accepted.
```

Configuring Community Strings (SNMPv1 and SNMPv2c Only)

To configure a community string for SNMPv1 or SNMPv2c, use the following command:

set snmp community name *comm-string*
access {read-only | read-notify | notify-only | read-write | notify-read-write}

The c*omm-string* can be up to 32 alphanumeric characters long, with no spaces. You can configure up to 10 community strings.

The access level specifies the read-write privileges of the community string:

- **read-only**—An SNMP management application using the string can get (read) object values on the switch but cannot set (write) them. This is the default.
- **read-notify**—An SNMP management application using the string can get object values on the switch but cannot set them. The switch can use the string to send notifications.
- **notify-only**—The switch can use the string to send notifications.
- **read-write**—An SNMP management application using the string can get and set object values on the switch.
- **notify-read-write**—An SNMP management application using the string can get and set object values on the switch. The switch can use the string to send notifications.

To clear an SNMP community string, use the following command:

clear snmp community name *comm-string*

The following command configures community string *switchmgr1* with access level **notify-read-write**:

```
23x0# set snmpsnmp community name switchmgr1 notify-read-write
success: change accepted.
```

Creating a USM User for SNMPv3

To create a USM user for SNMPv3, use the following command:

set snmp usm *usm-username*
snmp-engine-id {ip *ip-addr* | **local** | **hex** *hex-string*}
access {read-only | **read-notify** | **notify-only** | **read-write** | **notify-read-write}**
auth-type {none | **md5** | **sha}** {**auth-pass-phrase** *string* | **auth-key** *hex-string*}
encrypt-type {none | **des** | **3des** | **aes}** {**encrypt-pass-phrase** *string* |
encrypt-key *hex-string*}

To clear a USM user, use the following command:

clear snmp usm *usm-username*

The *usm-username* can be up to 32 alphanumeric characters long, with no spaces. You can configure up to 10 SNMPv3 users.

The **snmp-engine-id** option specifies a unique identifier for an instance of an SNMP engine. To send informs, you must specify the engine ID of the inform receiver. To send traps and to allow get and set operations and so on, specify **local** as the engine ID.

- **hex** *hex-string*—ID is a hexadecimal string.
- **ip** *ip-addr*—ID is based on the IP address of the station running the management application. Enter the IP address of the station. WSS Software calculates the engine ID based on the address.
- **local**—Uses the value computed from the switch's system IP address.

The **access** option specifies the access level of the user. The options are the same as the access options for community strings. (See "Configuring Community Strings (SNMPv1 and SNMPv2c Only)" on page 158.) The default is **read-only**.

The **auth-type** option specifies the authentication type used to authenticate communications with the remote SNMP engine. You can specify one of the following:

- **none**—No authentication is used. This is the default.
- **md5**—Message-digest algorithm 5 is used.
- **sha**—Secure Hashing Algorithm (SHA) is used.

If the authentication type is **md5** or **sha**, you can specify a passphrase or a hexadecimal key.

- To specify a passphrase, use the **auth-pass-phrase** *string* option. The string can be from 8 to 32 alphanumeric characters long, with no spaces.
- To specify a key, use the **auth-key** *hex-string* option.

The **encrypt-type** option specifies the encryption type used for SNMP traffic. You can specify one of the following:

- **none**—No encryption is used. This is the default.
- **des**—Data Encryption Standard (DES) encryption is used.
- **3des**—Triple DES encryption is used.
- **aes**—Advanced Encryption Standard (AES) encryption is used.

If the encryption type is **des**, **3des**, or **aes**, you can specify a passphrase or a hexadecimal key.

- To specify a passphrase, use the **encrypt-pass-phrase** *string* option. The string can be from 8 to 32 alphanumeric characters long, with no spaces.

- To specify a key, use the **encrypt-key** *hex-string* option.

Command Examples

The following command creates USM user *snmpmgr1*, associated with the local SNMP engine ID. This user can send traps to notification receivers.

```
23x0# set snmp usm snmpmgr1 snmp-engine-id local
success: change accepted.
```

The following command creates USM user *securesnmpmgr1*, which uses SHA authentication and 3DES encryption with passphrases. This user can send informs to the notification receiver that has engine ID 192.168.40.2.

```
23x0# set snmp usm securesnmpmgr1 snmp-engine-id ip 192.168.40.2 auth-type sha
    auth-pass-phrase myauthpword encrypt-type 3des encrypt-pass-phrase mycryptpword
success: change accepted.
```

Setting SNMP Security

By default, WSS Software allows nonsecure SNMP message exchanges. You can configure WSS Software to require secure SNMP exchanges instead.

Depending on the level of security you want WSS Software to enforce, you can require authentication of message exchanges only, or of message exchanges and notifications. You also can require encryption in addition to authentication.

SNMPv1 and SNMPv2c do not support authentication or encryption. If you plan to use SNMPv1 or SNMPv2c, leave the minimum level of SNMP security set to **unsecured**.

To set the minimum level of security WSS Software requires for SNMP, use the following command:

set snmp security {unsecured | authenticated | encrypted | auth-req-unsec-notify}

You can specify one of the following options:

- **unsecured**—SNMP message exchanges are not secure. This is the default, and is the only value supported for SNMPv1 and SNMPv2c. (This security level is the same as the noAuthNoPriv level described in SNMPv3 RFCs.)
- **authenticated**—SNMP message exchanges are authenticated but are not encrypted. (This security level is the same as the authNoPriv level described in SNMPv3 RFCs.)
- **encrypted**—SNMP message exchanges are authenticated and encrypted. (This security level is the same as the authPriv level described in SNMPv3 RFCs.)
- **auth-req-unsec-notify**—SNMP message exchanges are authenticated but are not encrypted, and notifications are neither authenticated nor encrypted.

Command Example

The following command sets the minimum level of SNMP security allowed to authentication ***and*** encryption:

```
23x0# set snmp security encrypted
success: change accepted.
```

Configuring a Notification Profile

A *notification profile* is a named list of all the notification types that can be generated by a switch, and for each notification type, the action to take (drop or send) when an event occurs.

A default notification profile (named *default*) is already configured in WSS Software. All notifications in the default profile are dropped by default. You can configure up to 10 notification profiles.

To modify the default notification profile or create a new one, use the following command:

set snmp profile {default | *profile-name*} {**drop** | **send**} {*notification-type* | **all**}

To clear a notification profile, use the following command:

clear snmp profile *profile-name*

The *profile-name* can be up to 32 alphanumeric characters long, with no spaces. To modify the default notification profile, specify **default**.

The *notification-type* can be one of the following:

- **AuthenTraps—**Generated when the WSS switch's SNMP engine receives a bad community string.
- **AutoTuneRadioChannelChangeTraps—**Generated when the RF Auto-Tuning feature changes the channel on a radio.
- **AutoTuneRadioPowerChangeTraps—**Generated when the RF Auto-Tuning feature changes the power setting on a radio.
- **ClientAssociationFailureTraps—**Generated when a client's attempt to associate with a radio fails.
- **ClientAuthorizationSuccessTraps—**Generated when a client is successfully authorized.
- **ClientAuthenticationFailureTraps—**Generated when authentication fails for a client.
- **ClientAuthorizationFailureTraps—**Generated when authorization fails for a client.
- **ClientClearedTraps—**Generated when a client's session is cleared.
- **ClientDeAssociationTraps—**Generated when a client is dissociated from a radio.
- **ClientDot1xFailureTraps—**Generated when a client experiences an 802.1X failure.
- **ClientRoamingTraps—**Generated when a client roams.
- **CounterMeasureStartTraps—**Generated when WSS Software begins countermeasures against a rogue access port.
- **CounterMeasureStopTraps—**Generated when WSS Software stops countermeasures against a rogue access port.
- **DAPConnectWarningTraps**—generated when a Distributed AP whose fingerprint has not been configured in WSS Software establishes a management session with the switch.
- **DeviceFailTraps—**Generated when an event with an Alert severity occurs.
- **DeviceOkayTraps—**Generated when a device returns to its normal state.
- **LinkDownTraps—**Generated when the link is lost on a port.
- **LinkUpTraps—**Generated when the link is detected on a port.
- **MichaelMICFailureTraps—**Generated when two Michael message integrity code (MIC) failures occur within 60 seconds, triggering Wi-Fi Protected Access (WPA) countermeasures.
- **MobilityDomainJoinTraps—**Generated when the WSS switch is initially able to contact a mobility domain seed member, or can contact the seed member after a timeout.

- **MobilityDomainTimeoutTraps—**Generated when a timeout occurs after an WSS switch has unsuccessfully tried to communicate with a seed member.
- **APBootTraps—**Generated when an AP access point boots.
- **APTimeoutTraps—**Generated when an AP access point fails to respond to the WSS switch.
- **PoEFailTraps—**Generated when a serious PoE problem, such as a short circuit, occurs.
- **RFDetectAdhocUserTraps**—Generated when WSS Software detects an ad-hoc user.
- **RFDetectRogueAPTraps**—Generated when MS detects a rogue access port.
- **RFDetectRogueDisappearTraps**—Generated when a rogue access point is no longer being detected.
- **RFDetectClientViaRogueWiredAPTraps**—Generated when WSS Software detects, on the wired part of the network, the MAC address of a wireless client associated with a third-party AP.
- **RFDetectDoSPortTraps**—Generated when WSS Software detects an associate request flood, reassociate request flood, or disassociate request flood.
- **RFDetectDoSTraps**—Generated when WSS Software detects a DoS attack other than an associate request flood, reassociate request flood, or disassociate request flood.
- **RFDetectInterferingRogueAPTraps**—Generated when an interfering device is detected.
- **RFDetectInterferingRogueDisappearTraps**—Generated when an interfering device is no longer detected.
- **RFDetectSpoofedMacAPTraps**—Generated when WSS Software detects a wireless packet with the source MAC address of a Nortel AP, but without the spoofed AP's signature (fingerprint).
- **RFDetectSpoofedSsidAPTraps**—Generated when WSS Software detects beacon frames for a valid SSID, but sent by a rogue AP.
- **RFDetectUnAuthorizedAPTraps**—Generated when WSS Software detects the MAC address of an AP that is on the attack list.
- **RFDetectUnAuthorizedOuiTraps**—Generated when a wireless device that is not on the list of permitted vendors is detected.
- **RFDetectUnAuthorizedSsidTraps**—Generated when an SSID that is not on the permitted SSID list is detected.

To apply the configuration change to all notification types, specify **all**.

The **drop** or **send** option specifies the action that the SNMP engine takes with regard to notifications.

Command Examples

The following command changes the action in the default notification profile from **drop** to **send** for all notification types:

```
23x0# set snmp notify profile default send all
success: change accepted.
```

The following commands create notification profile *snmpprof_rfdetect*, and change the action to **send** for all RF detection notification types:

```
23x0# set snmp notify profile snmpprof_rfdetect send RFDetectAdhocUserTraps
success: change accepted.
```

```
23x0# set snmp notify profile snmpprof_rfdetect send
    RFDetectClientViaRogueWiredAPTraps
success: change accepted.

23x0# set snmp notify profile snmpprof_rfdetect send RFDetectDoSTraps
success: change accepted.

23x0# set snmp notify profile snmpprof_rfdetect send RFDetectAdhocUserTraps
success: change accepted.

23x0# set snmp notify profile snmpprof_rfdetect send
    RFDetectInterferingRogueAPTraps
success: change accepted.

23x0# set snmp notify profile snmpprof_rfdetect send
    RFDetectInterferingRogueDisappearTraps
success: change accepted.

23x0# set snmp notify profile snmpprof_rfdetect send RFDetectRogueAPTraps
success: change accepted.

23x0# set snmp notify profile snmpprof_rfdetect send
    RFDetectRogueDisappearTraps
success: change accepted.

23x0# set snmp notify profile snmpprof_rfdetect send
    RFDetectSpoofedMacAPTraps
success: change accepted.

23x0# set snmp notify profile snmpprof_rfdetect send
    RFDetectSpoofedSsidAPTraps
success: change accepted.

23x0# set snmp notify profile snmpprof_rfdetect send
    RFDetectUnAuthorizedAPTraps
success: change accepted.

23x0# set snmp notify profile snmpprof_rfdetect send
    RFDetectUnAuthorizedOuiTraps
success: change accepted.

23x0# set snmp notify profile snmpprof_rfdetect send
    RFDetectUnAuthorizedSsidTraps
success: change accepted.
```

Configuring a Notification Target

A notification target is a remote device to which WSS Software sends SNMP notifications. You can configure the WSS Software SNMP engine to send confirmed notifications (informs) or unconfirmed notifications (traps). Some of the command options differ depending on the SNMP version and the type of notification you specify. You can configure up to 10 notification targets.

To configure a notification target for informs from SNMPv3, use the following command:

set snmp notify target *target-num ip-addr*[**:***udp-port-number*]
usm inform user *username*
snmp-engine-id {**ip** | **hex** *hex-string*}
[**profile** *profile-name*]
[**security** {**unsecured** | **authenticated** | **encrypted**}]
[**retries** *num*]
[**timeout** *num*]

To configure a notification target for traps from SNMPv3, use the following command:

set snmp notify target *target-num ip-addr*[**:***udp-port-number*]
usm trap user *username*
[**profile** *profile-name*]
[**security** {**unsecured** | **authenticated** | **encrypted**}]

To configure a notification target for informs from SNMPv2c, use the following command:

set snmp notify target *target-num ip-addr*[**:***udp-port-number*]
v2c *community-string* **inform**
[**profile** *profile-name*]
[**retries** *num*]
[**timeout** *num*]

To configure a notification target for traps from SNMPv2c, use the following command:

set snmp notify target *target-num ip-addr*[**:***udp-port-number*]
v2c *community-string* **trap**
[**profile** *profile-name*]

To configure a notification target for traps from SNMPv1, use the following command:

set snmp notify target *target-num ip-addr*[**:***udp-port-number*]
v1 *community-string*
[**profile** *profile-name*]

To clear a notification target, use the following command:

clear snmp notify target *target-num*

The *target-num* is an ID for the target. This ID is local to the WSS switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.

The *ip-addr*[**:***udp-port-number*] is the IP address of the server. You also can specify the UDP port number to send notifications to. The default is 162.

Use **v1**, **v2c**, or **usm** to specify the SNMP version.

The **inform** or **trap** option specifies whether the WSS Software SNMP engine expects the target to acknowledge notifications sent to the target by the WSS switch. Use **inform** if you want acknowledgements. Use **trap** if you do not want acknowledgements. The **inform** option is applicable to SNMP version **v2c** or **usm** only.

The *username* is a USM username, and is applicable only when the SNMP version is **usm**. If the user will send informs rather than traps, you also must specify the **snmpSNMP-engine-id** of the target. Specify **ip** if the target's SNMP engine ID is based on its IP address. If the target's SNMP engine ID is a hexadecimal value, use **hex** *hex-string* to specify the value.

The *community-string* is applicable only when the SNMP version is **v1** or **v2c**.

The *profile-name* is the notification profile. The default is **default**.

The **security** option specifies the security level, and is applicable only when the SNMP version is **usm**:

- **unsecured**—Message exchanges are not authenticated, nor are they encrypted. This is the default.
- **authenticated**—Message exchanges are authenticated, but are not encrypted.
- **encrypted**—Message exchanges are authenticated and encrypted.

The **retries** and **timeout** options are applicable only when the SNMP version is **v2c** or **usm** and the notification type is **inform**. The **retries** option specifies the number of times the WSS Software SNMP engine will resend a notification that has not been acknowledged by the target. You can specify from 0 to 3 retries. The default is 0. The **timeout** option specifies the number of seconds WSS Software waits for acknowledgement of a notification. You can specify from 1 to 5 seconds. The default is 2.

Command Examples

The following command configures a notification target for acknowledged notifications:

```
23x0# set snmp notify target 1 10.10.40.9 usm inform user securesnmpmgr1 snmp-engine-id
    ip
success: change accepted.
```

This command configures target 1 at IP address 10.10.40.9. The target's SNMP engine ID is based on its address. The WSS Software SNMP engine will send notifications based on the default profile, and will require the target to acknowledge receiving them.

The following command configures a notification target for unacknowledged notifications:

```
23x0# set snmp notify target 2 10.10.40.10 v1 trap
success: change accepted.
```

Enabling the SNMP Service

To enable the WSS Software SNMP service, use the following command:

set ip snmp server {enable | disable}

The following command enables the SNMP service:

```
23x0# set ip snmp server enable
success: change accepted.
```

Displaying SNMP Information

You can display the following SNMP information:

- Version and status information
- Configured community strings
- User-based security model (USM) settings
- Notification targets
- SNMP statistics counters

Displaying SNMP Version and Status Information

To display SNMP version and status information, use the following command:

```
23x0# show snmp status
<<insert updated example>>
```

Displaying the Configured SNMP Community Strings

To display the configured SNMP community strings, use the following command:

```
23x0# show snmp community
<<insert updated example>>
```

Displaying USM Settings

To display USM settings, use the following command:

```
23x0# show snmp usm
<<insert updated example>>
```

Displaying Notification Profiles

To display notification profiles, use the following command:

```
23x0# show snmp notify profile
<<insert updated example>>
```

The command lists settings separately for each notification profile. The use count indicates how many notification targets use the profile. For each notification type, the command lists whether WSS Software sends notifications of that type to the targets that use the notification profile.

Displaying Notification Targets

To display a list of the SNMP notification targets, use the following command:

```
23x0# show snmp notify target
<<insert updated example>>
```

Displaying SNMP Statistics Counters

To display SNMP statistics counters, use the following command:

```
23x0# show snmp counters
<<insert updated example>>
```

Configuring and Managing Mobility Domain Roaming

About the Mobility Domain Feature 175
Configuring a Mobility Domain 176
Monitoring the VLANs and Tunnels in a Mobility Domain 183
Understanding the Sessions of Roaming Users 186
Mobility Domain Scenario 189

A Mobility Domain is a system of WSSs and AP access points working together to support roaming wireless users (clients). Tunnels and virtual ports between the WSSs in a Mobility Domain allow users to roam without any disruption to network connectivity.

(If your Mobility Domain uses firewalls or access controls between WSSs or AAA servers, see Appendix , “Mobility Domain Traffic Ports,” on page 605 for the ports typically used in a Mobility Domain.)



Note. Nortel recommends that you run the same WSS Software version on all the WSSs in a Mobility Domain.

About the Mobility Domain Feature

A Mobility Domain enables users to roam geographically across the system while maintaining their data sessions and VLAN or subnet membership, including IP address, regardless of how the WSS switches are attached to the network backbone. As users move from one area of a building or campus to another, their association with servers or other resources appears the same.

When users access a WSS in a Mobility Domain, they become members of the VLAN designated through their authorized identity. If a user’s native VLAN is not present on the WSS that he or she accesses, the accessed WSS forms a tunnel to an WSS in the Mobility Domain that includes the native VLAN.

In a Mobility Domain, one WSS acts as a seed device, which distributes information to the WSSs defined in the Mobility Domain. Otherwise, the seed WSS operates like any other Mobility Domain member.

Configuring a Mobility Domain

The WSSs in a Mobility Domain use their system IP address for Mobility Domain communication. To support the services of the Mobility Domain, the system IP address of every WSS requires basic IP connectivity to the system IP address of every other WSS. (For information about setting the system IP address for the WSS, see "Configuring the System IP Address" on page 114.)

To create a Mobility Domain:

1. Designate a seed WSS. (See "Configuring the Seed" on page 177.)
2. Create a list of the member WSSs. (See "Configuring Member WSSs on the Seed" on page 178.)
3. Configure each member WSS to point to the seed. (See "Configuring a Member" on page 179.)

You can view the status and configuration of a Mobility Domain, clear members, and clear all Mobility Domain configuration from a WSS.

Configuring the Seed

You must explicitly configure *only one* WSS per domain as the seed. All other WSS switches in the domain receive their Mobility Domain information from the seed.

Use the following command to set the current WSS switch as the seed device and name the Mobility Domain:

set mobility-domain mode seed domain-name *mob-domain-name*

For example, the following command sets the current WSS as the seed and names the Mobility Domain *Pleasanton*:

```
23x0# set mobility-domain mode seed domain-name Pleasanton
success: change accepted.
```

The Mobility Domain name is assigned to the seed WSS only. The WSS system IP address is used as the source IP address for all Mobility Domain communications. If the system IP address is not set, WSS Software issues a warning when you enter the **set mobility-domain mode seed** *domain-name* command, to inform you that the Mobility Domain is not operational until the system IP is set.

Configuring Member WSSs on the Seed

To configure the list of members on the Mobility Domain seed for distribution to other member WSSs, use the following command on the seed WSS:

set mobility-domain member *ip-addr*

For example, the following commands add two members with IP addresses 192.168.12.7 and 192.168.15.5 to a Mobility Domain whose seed is the current WSS:

```
23x0# set mobility-domain member 192.168.12.7
success: change accepted.

23x0# set mobility-domain member 192.168.15.5
success: change accepted.
```

Each command adds a member identified by its IP address to the list of Mobility Domain members. If the WSS from which you enter the command is not configured as a seed, the command is rejected.

Configuring a Member

To configure a member WSS in the Mobility Domain, you enter the following command when logged in to the nonseed member WSS:

set mobility-domain mode member seed-ip *ip-addr*

This command configures the IP destination address that the member WSS uses when communicating with the seed WSS switch.

For example, the following command configures the current WSS as a member of the Mobility Domain whose seed is 192.168.253.6:

```
23x0# set mobility-domain mode member seed-ip 192.168.253.6
success: change accepted.
```

This command sets the WSS as a member of the Mobility Domain defined on the seed device at the identified address. If the WSS is currently part of another Mobility Domain or using another seed, this command overwrites that configuration. After you enter this command, the member WSS obtains a new list of members from its new seed's IP address.

Displaying Mobility Domain Status

To view the status of the Mobility Domain for the WSS, use the **show mobility-domain status** command. For example:

```
2370# show mobility-domain status
Mobility Domain name:  Pleasanton
Member              State             Status
--------------      -------------     --------------
192.168.12.7        STATE_UP          MEMBER
192.168.14.6        STATE_UP          SEED
192.168.15.5        STATE_UP          MEMBER
```

Displaying the Mobility Domain Configuration

To view the configuration of the Mobility Domain, use the **show mobility-domain config** command on either the seed or a nonseed member.

- To view Mobility Domain configuration on the seed:

```
2370# show mobility-domain config
This WSS is the seed for domain Pleasanton.
192.168.12.7 is a member
192.168.15.5 is a member
```

- To view Mobility Domain configuration on a member:

```
2370# show mobility-domain config
This WSS is a member, with seed 192.168.14.6
```

Clearing a Mobility Domain from a WSS

You can clear all Mobility Domain configuration from a WSS , regardless of whether the WSS is a seed or a member of a Mobility Domain.

You might want to clear the Mobility Domain to change a WSS from one Mobility Domain to another, or to remove a WSS from the Mobility Domain. To clear the Mobility Domain, type the following command:

```
2370# clear mobility-domain
success: change accepted
```

This command has no effect if the WSS is not configured as part of a Mobility Domain.

Clearing a Mobility Domain Member from a Seed

You can remove individual members from the Mobility Domain on the seed WSS. To remove a specific member of the Mobility Domain, type the following command:

clear mobility-domain member *ip-addr*

This command has no effect if the WSS member is not configured as part of a Mobility Domain or the current WSS is not the seed.

Monitoring the VLANs and Tunnels in a Mobility Domain

Tunnels connect WSSs. Tunnels are formed automatically in a Mobility Domain to extend a VLAN to the WSS that a roaming station is associated with. A single tunnel can carry traffic for many users and many VLANs. The tunnel port can carry traffic for multiple VLANs by means of multiple *virtual ports*.

WSS Software automatically adds virtual ports to VLANs as needed to preserve the associations of users to the correct subnet or broadcast domain as they roam across the Mobility Domain. Although tunnels are formed by IP between WSSs, the tunnels can carry user traffic of any protocol type.

WSS Software provides the following commands to display the roaming and tunneling of users within their Mobility Domain groups:

- **show roaming station** (See "Displaying Roaming Stations" on page 184.)
- **show roaming vlan** (See "Displaying Roaming VLANs and Their Affinities" on page 185.)
- **show tunnel** (See "Displaying Tunnel Information" on page 186.)

Displaying Roaming Stations

The command **show roaming station** displays a list of the stations roaming to the WSS switch through a VLAN tunnel. To display roaming stations (clients), type the following command:

23x0# **show roaming station**

```
User Name              Station Address   Old AP MAC        VLAN            State
---------------------- ----------------- ----------------- --------------- -----
example\geetha         192.168.15.104 00:00:00:00:00:00   vlan-am         Up
nh@example.com         192.168.15.199 00:00:00:00:00:00   vlan-am         Up
example\tamara         192.168.11.200 00:00:00:00:00:00   vlan-ds         Up
example\jose           192.168.14.200 00:00:00:00:00:00   vlan-et         Up
hh@example.com         192.168.15.194 00:00:00:00:00:00   vlan-am         Up
```

(For more information about this command and the fields in the output, see the *Nortel Mobility System Software Command Referenc*e.)

Displaying Roaming VLANs and Their Affinities

The command **show roaming vlan** displays all VLANs in the Mobility Domain, the WSSs servicing the VLANs, and their tunnel *affinity* values configured on each switch for the VLANs.

The member WSS that offers the requested VLAN reports the affinity number. If multiple WSSs have native attachments to the VLAN, the affinity values they advertise are a way to attract tunneled traffic to a particular WSS for that VLAN. A higher value represents preferred connection to the VLAN. (For more information, see "Changing Tunneling Affinity" on page 95.)

To display roaming VLANs, type the following command:

```
23x0# show roaming vlan
VLAN             WSS               Affinity
---------------- ---------------- --------
vlan-eng         192.168.12.7            5
vlan-fin         192.168.15.5            5
vlan-pm          192.168.15.5            5
vlan-wep         192.168.12.7            5
vlan-wep         192.168.15.5            5
```

(For more information about this command and the fields in the output, see th*e Nortel Mobility System Software Command Reference.)*

Displaying Tunnel Information

The command **show tunnel** displays the tunnels that the WSS switch is hosting to distribute to a locally attached VLAN. To display tunnel information, type the following command:

```
23x0# show tunnel
VLAN          Local Address   Remote Address  State   Port  LVID  RVID
------------------------------------------------------------------ ---
vlan-eng       192.168.12.7    192.168.15.5    UP      1024   130  4103
vlan-eng      192.168.12.7    192.168.14.6    DORMANT  1026   130  4097
vlan-pm        192.168.12.7    192.168.15.5    UP      1024  4096   160
```

(For more information about this command and the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

Understanding the Sessions of Roaming Users

When a wireless client successfully roams from one AP to another, its sessions are affected in the following ways:

- The WSS treats this client session as a roaming session and not a new session.
- RADIUS accounting is handled as a continuation of an existing session, rather than a new one.
- The session with the roamed-from AP is cleared from the WSS, even if the client does not explicitly disassociate from the AP and the IEEE 802.1X reauthentication period has not expired.

Roaming requires certain conditions and can be affected by some of the WSS's timers. You can monitor a wireless client's roaming sessions with the **show sessions network verbose** command.

Requirements for Roaming to Succeed

For roaming to take place, the roaming client must associate or reassociate with an AP in the Mobility Domain after leaving an existing session on a different AP in the Mobility Domain in one of the following states:

ACTIVE	The normal state for a client that has left radio range without sending a request to disassociate.
DEASSOCIATED	The state of a client that has sent an 802.11 disassociate message, but has not roamed or aged out yet.

In addition, the following conditions must exist for roaming to succeed:

- Mobility Domain communications must be stable.

  Generally, the communications required for roaming are the same as those required for VLAN tunneling. A client can also roam among ports on a WSS when a Mobility Domain is inaccessible or not configured.

- Client authentication and authorization on the roamed-to AP must be successful on the first attempt.

  If authentication or authorization fails, WSS Software clears the client session. Depending on when the failure occurs, roaming can be disqualified or delayed.

- The client must use the same authorization parameters for the roamed-to AP as for the roamed-from AP.

  If the client changes its encryption type or VLAN name, WSS Software might record a new session rather than a roamed session.

Effects of Timers on Roaming

An unsuccessful roaming attempt might be caused by the following timers. You cannot configure either timer.

- **Grace period.** A disassociated session has a grace period of 5 seconds during which WSS Software can retrieve and forward the session history. After 5 seconds, WSS Software clears the session, and its accounting is stopped.
- **MAC address search.** If WSS Software cannot find the client's MAC address in a Mobility Domain within 5 seconds, it treats the session as a new session rather than a roaming session.

In contrast, the 802.1X reauthentication timeout period has little effect on roaming. If the timeout expires, WSS Software performs 802.1X processing on the existing association. Accounting and roaming history are unaffected when reauthentication is successful, because the client is still associated with the same AP. If reauthentication fails, WSS Software clears the session so it is not eligible for roaming.

If the client associates with the same AP, the session is recorded as a new session.

(To change the reauthentication timeout, see "Setting the 802.1X Reauthentication Period" on page 498.)

Monitoring Roaming Sessions

To monitor the state of roaming clients, use the **show sessions network verbose** command. For example, the following command displays information about the sessions of a wireless client who roamed between the ports on an WSS switch.

The output shows that the client *SHUTTLE\2\exAPl* roamed from the AP access point connected to port 3 to the AP connected to port 6 on the same WSS, and then roamed back to the AP connected to port 3.

```
WSS-20> show sessions network verbose
User                            Sess  IP or MAC         VLAN            Port/
Name                              ID  Address           Name            Radio
------------------------------ ----  ----------------- --------------- -----
SHUTTLE2\exAPl                   6* 10.3.8.55         default         3/1
Client MAC: 00:06:25:13:08:33   GID: SESS-4-000404-98441-c807c14b
State: ACTIVE                  (prev AUTHORIZED)
now on: WSS 10.3.8.103, AP/radio  3/1, AP 00:0b:0e:ff:00:3a, as of
00:00:24 ago
  from: WSS 10.3.8.103, AP/radio  6/1, AP 00:0b:0e:00:05:d7, as of
00:01:07 ago
  from: WSS 10.3.8.103, AP/radio  3/1, AP 00:0b:0e:ff:00:3a, as of
00:01:53 ago

1 sessions total
```

(For more information about this command and the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

Mobility Domain Scenario

The following scenario illustrates how to create a Mobility Domain named *sunflower* consisting of three members from a seed WSS switch at 192.168.253.21:

1. Make the current WSS the Mobility Domain seed. Type the following command:

   ```
   23x0# set mobility-domain mode seed domain-name sunflower
   success: change accepted.
   ```

2. On the seed, add the members of the Mobility Domain. Type the following commands:

   ```
   23x0# set mobility-domain member 192.168.253.11
   success: change accepted.
   ```

   ```
   23x0# set mobility-domain member 192.168.111.112
   success: change accepted.
   ```

3. For each member WSS, configure the IP address used to reach the seed WSS. Type the following commands:

   ```
   23x0# set mobility-domain member seed-ip 192.168.253.21
   ```

4. Display the Mobility Domain status. Type the following command:

   ```
   23x0# show mobility-domain status
   Mobility Domain name:  sunflower
   Member              State             Status
   ```

```
---------------     -------------     --------------
192.168.111.112     STATE_UP          MEMBER
192.168.253.11      STATE_UP          MEMBER
192.168.253.21      STATE_UP          SEED
```

5 To display the Mobility Domain configuration, type the following command:

```
23x0# show mobility-domain config
This WSS is the seed for domain sunflower.
192.168.253.11 is a member
192.168.111.112 is a member
```

6 To display the WSS switches that are hosting VLANs for roaming, type the following command:

```
23x0# show roaming vlan
VLAN              WSS               Affinity
----------------- ----------------- --------
vlan-eng          192.168.12.7             5
vlan-fin          192.168.15.5             5
vlan-pm           192.168.15.5             5
vlan-wep          192.168.12.7             5
vlan-wep          192.168.15.5             5
```

7 To display active roaming tunnels, type the following command:

```
23x0# show tunnel
VLAN          Local Address   Remote Address  State   Port  LVID  RVID
-------------------------------------------------------------------------
vlan-eng       192.168.12.7   192.168.15.5   UP      1025  130  4096
vlan-eng       192.168.12.7   192.168.14.6   UP      1024  130  4096
```

Configuring User Encryption

Configuring WPA 194
Configuring WEP 209
Encryption Configuration Scenarios 212

WLAN 2300 System Software (WSS Software) encrypts wireless user traffic for all users who are successfully authenticated to join an encrypted SSID and who are then authorized to join a VLAN. WSS Software supports the following types of encryption for wireless user traffic:

- 802.11i
- Wi-Fi Protected Access (WPA)
- Non-WPA dynamic Wired Equivalent Privacy (WEP)
- Non-WPA static WEP

WEP is described in the IEEE 802.11 standard and WPA is described in the 802.11i standard.

WPA and 802.11i provide stronger security than WEP. (802.11i uses *Robust Security Network (RSN)*, and is sometimes called *WPA2*.)

To use WPA or RSN, a client must support it. For non-WPA clients, WSS Software supports WEP. If your network contains a combination of WPA, RSN, clients and non-WPA clients, you can configure WSS Software to provide encryption for both types of clients.

To configure encryption parameters for an SSID, create or edit a service profile, map the service profile to a radio profile, and add radios to the radio profile. The SSID name, advertisement setting (beaconing), and encryption settings are configured in the service profile.

You can configure an SSID to support any combination of WPA, RSN, and non-WPA clients. For example, a radio can simultaneously use Temporal Key Integrity Protocol (TKIP) encryption for WPA clients and WEP encryption for non-WPA clients.

The SSID type must be crypto (encrypted) for encryption to be used. If the SSID type is clear, wireless traffic is not encrypted, regardless of the encryption settings.



Note. WSS Software does not encrypt traffic in the wired part of the network. WSS Software does not encrypt wireless or wired traffic for users who associate with an unencrypted (clear) SSID.

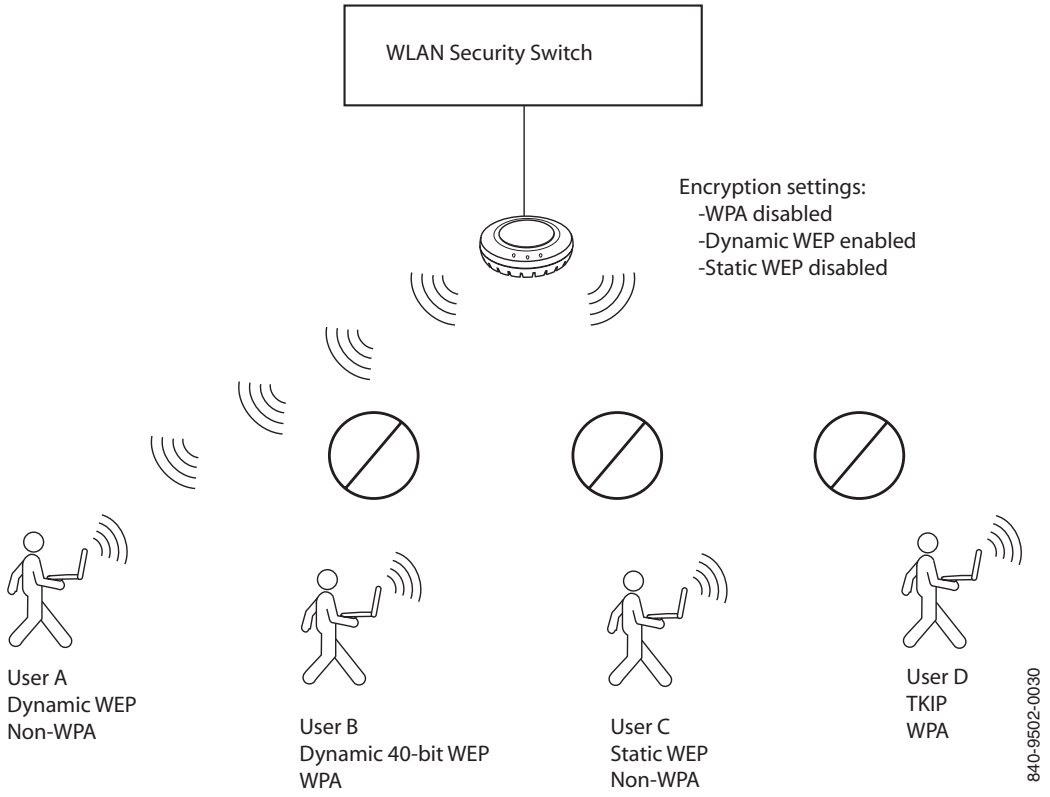
Table 5 on page 192 lists the encryption types supported by WSS Software and their default states.

Table 5: Wireless Encryption Defaults

Encryption Type	Client Support	Default State	Configuration Required in WSS Software
RSN	RSN clients Non-RSN clients	Disabled	• Enable the RSN information element (IE). • Specify the supported cipher suites (CCMP, TKIP, 40-bit WEP, 104-bit WEP). TKIP is enabled by default when the RSN IE is enabled.
WPA	WPA clients Non-WPA clients	Disabled	• Enable the WPA information element (IE). • Specify the supported cipher suites (CCMP, TKIP, 40-bit WEP, 104-bit WEP). TKIP is enabled by default when the WPA IE is enabled.
Dynamic WEP	WEP clients (WPA and RSN not supported)	Enabled	None
Static WEP	WEP clients (WPA and RSN not supported)	Disabled	• Configure the static key(s). • Assign keys to multicast and unicast traffic.

Figure 2 shows the client support when the default encryption settings are used. A radio using the default encryption settings encrypts traffic for non-WPA dynamic WEP clients but not for WPA clients or static WEP clients. The radio disassociates from these other clients.

Figure 2. Default Encryption



This rest of this chapter describes the encryption types and how to configure them, and provides configuration scenarios.

Configuring WPA

Wi-Fi Protected Access (WPA) is a security enhancement to the IEEE 802.11 wireless standard. WPA provides enhanced encryption with new cipher suites and provides per-packet message integrity checks. WPA is based on the 802.11i standard. You can use WPA with 802.1X authentication. If the client does not support 802.1X, you can use a preshared key on the AP access point and the client for authentication.

WPA Cipher Suites

WPA supports the following cipher suites for packet encryption, listed from most secure to least secure:

- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)—CCMP provides Advanced Encryption Standard (AES) data encryption. To provide message integrity, CCMP uses the Cipher Block Chaining Message Authentication Code (CBC-MAC).
- Temporal Key Integrity Protocol (TKIP)—TKIP uses the RC4 encryption algorithm, a 128-bit encryption key, a 48-bit initialization vector (IV), and a message integrity code (MIC) called Michael.
- Wired Equivalent Privacy (WEP) with 104-bit keys—104-bit WEP uses the RC4 encryption algorithm with a 104-bit key.
- WEP with 40-bit keys—40-bit WEP uses the RC4 encryption algorithm with a 40-bit key.

You can configure AP access ports to support one or more of these cipher suites. For all of these cipher suites, WSS Software dynamically generates unique session keys for each session. WSS Software periodically changes the keys to reduce the likelihood that a network intruder can intercept enough frames to decode a key.

Figure 3 shows the client support when WPA encryption for TKIP only is enabled. A radio using WPA with TKIP encrypts traffic only for WPA TKIP clients but not for CCMP or WEP clients. The radio disassociates from these other clients.

Figure 3. WPA Encryption with TKIP Only

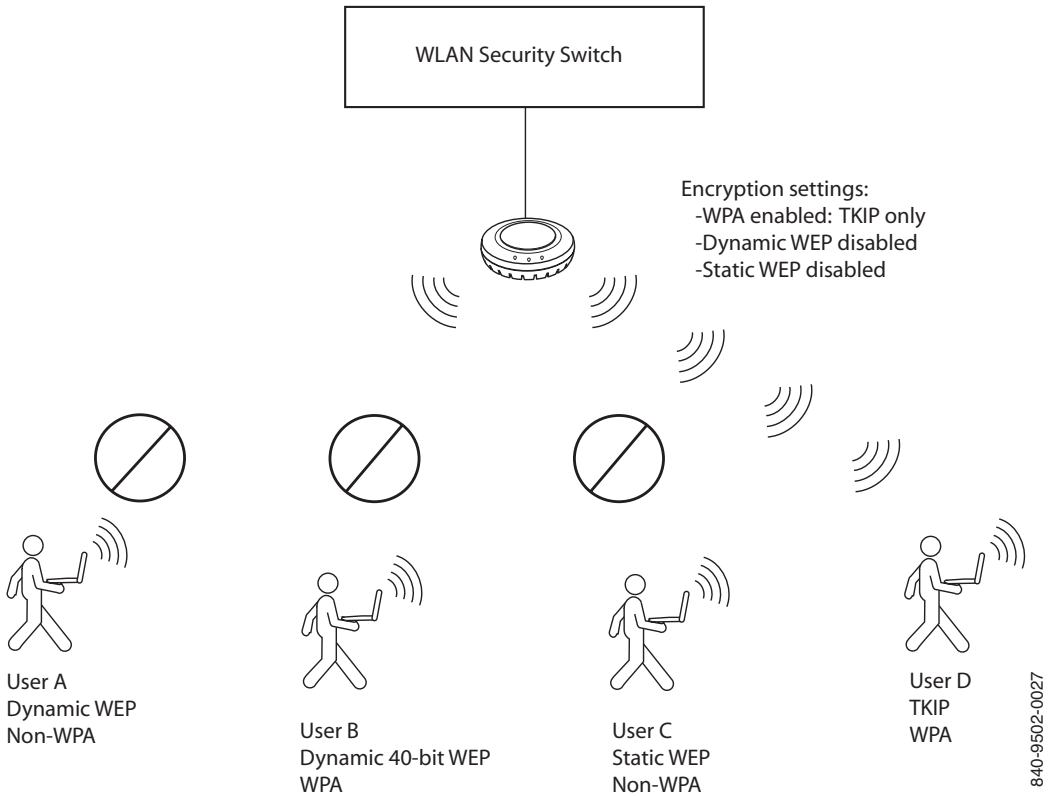
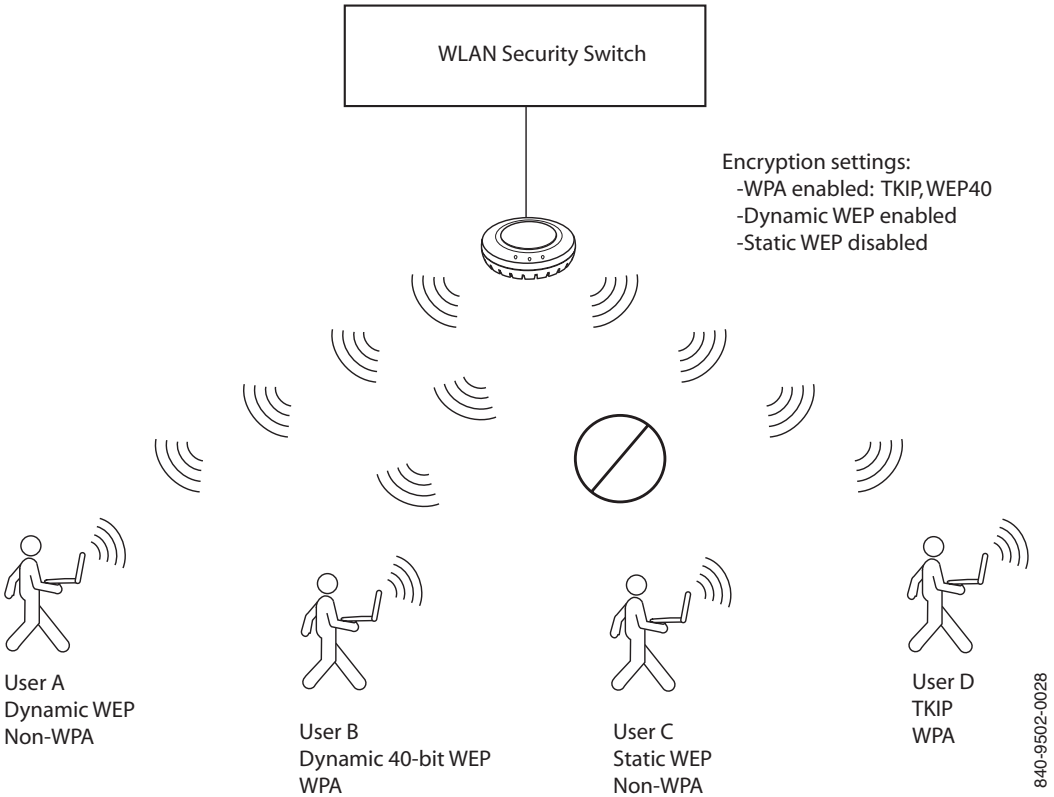


Figure 4 shows the client support when both WEP encryption and TKIP are enabled. A radio using WPA with TKIP and WEP encrypts traffic for WPA TKIP clients, WPA WEP clients, *and* non-WPA dynamic WEP clients, but not for CCMP or static WEP clients. The radio disassociates from these other clients.

Figure 4. WPA Encryption with TKIP and WEP



TKIP Countermeasures

WPA access ports and clients verify the integrity of a wireless frame received on the network by generating a keyed message integrity check (MIC). The Michael MIC used with TKIP provides a holddown mechanism to protect the network against tampering.

- If the recalculated MIC matches the MIC received with the frame, the frame passes the integrity check and the access point or client processes the frame normally.
- If the recalculated MIC does not match the MIC received with the frame, the frame fails the integrity check. This condition is called a MIC failure. The access point or client discards the frame and also starts a 60-second timer. If another MIC failure does not occur within 60 seconds, the timer expires. However, if another MIC failure occurs before the timer expires, the device takes the following actions:

    - An AP access point that receives another frame with an invalid MIC ends its sessions with all TKIP and WEP clients by disassociating from the clients. This includes both WPA WEP clients and non-WPA WEP clients. The access point also temporarily shuts down the network by refusing all association or reassociation requests from TKIP and WEP clients. In addition, WSS Software generates an SNMP trap that indicates the WSS port and radio that received frames with the two MIC failures as well as the source and destination MAC addresses in the frames.
    - A client that receives another frame with an invalid MIC disassociates from its access point and does not send or accept any frames encrypted with TKIP or WEP.

    The AP access point or client refuses to send or receive traffic encrypted with TKIP or WEP for the duration of the countermeasures timer, which is 60,000 milliseconds (60 seconds) by default. When the countermeasures timer expires, the access point allows associations and reassociations and generates new session keys for them. You can set the countermeasures timer for AP access point radios to a value from 0 to 60,000 milliseconds (ms). If you specify 0 ms, the radios do not use countermeasures but instead continue to accept and forward encrypted traffic following a second MIC failure. However, WSS Software still generates an SNMP trap to inform you of the MIC failure.

The MIC used by CCMP, CBC-MAC, is even stronger than Michael and does not require or provide countermeasures. WEP does not use a MIC. Instead, WEP performs a cyclic redundancy check (CRC) on the frame and generates an integrity check value (ICV).

WPA Authentication Methods

You can configure an SSID to support one or both of the following authentication methods for WPA clients:

- 802.1X—The AP access point and client use an Extensible Authentication Protocol (EAP) method to authenticate one another, then use the resulting key in a handshake to derive a unique key for the session. The 802.1X authentication method requires user information to be configured on AAA servers or in the WSS switch's local database. This is the default WPA authentication method.
- Preshared key (PSK)—An AP radio and a client authenticate one another based on a key that is statically configured on both devices. The devices then use the key in a handshake to derive a unique key for the session. For a given service profile, you can globally configure a PSK for use with all clients. You can configure the key by entering an ASCII passphrase or by entering the key itself in raw (hexadecimal) form.



Note. For a MAC client that authenticates using a PSK, the RADIUS servers or local database still must contain an authentication rule for the client, to assign the client to a VLAN.



Note. The Web-based AAA fallthru authentication type is not supported in conjunction with WPA encryption using preshared keys (PSK) for the same SSID. These options are configurable together but are not compatible. Web-based AAA traffic is not encrypted, whereas the PSK four-way handshake requires a client to already be authenticated and for encryption to be in place.

WPA Information Element

A WPA information element (IE) is a set of extra fields in a wireless frame that contain WPA information for the access point or client. To enable WPA support in a service profile, you must enable the WPA IE. The following types of wireless frames can contain a WPA IE:

- Beacon (sent by an AP access port)—The WPA IE in a beacon frame advertises the cipher suites and authentication methods that an AP radio supports for the encrypted SSID. The WPA IE also lists the cipher suites that the radio uses to encrypt broadcast and multicast frames. An AP radio always uses the least secure of the cipher suites to encrypt broadcast and multicast frames to ensure that all clients associated with the SSID can decrypt the frames. An AP radio uses the most secure cipher suite supported by both the radio and a client to encrypt unicast traffic to that client.
- Probe response (sent by an AP radio)—The WPA IE in a probe response frame lists the same WPA information that is contained in the beacon frame.
- Association request or reassociation (sent by a client)—The WPA IE in an association request lists the authentication method and cipher suite the client wants to use.

Client Support

To use the TKIP or CCMP cipher suite for encryption, a client must support WPA. However, an AP radio configured for WPA can support non-WPA clients who use dynamic WEP or static WEP. If the WPA IE is enabled in the service profile used by an SSID supported by the radio, and the 40-bit WEP or 104-bit WEP cipher suite also is enabled in the service profile, WSS Software allows a non-WPA client to authenticate using WEP under the following circumstances:

- If a client wants to authenticate using dynamic WEP, WSS Software uses 802.1X to authenticate the client if either the WEP40 or WEP104 cipher suite is enabled for WPA.
- If a client wants to authenticate using static WEP, the radio checks for the static WEP key presented by the client. If the keys match, WSS Software authenticates the client. Because the WEP key is static, WSS Software does not use 802.1X to authenticate the client.

To allow a non-WPA client that uses dynamic WEP to be authenticated by a radio on which WPA IE is enabled, enable the WEP40 or WEP104 cipher suite in the service profile for the SSID the client will access. To prevent non-WPA clients that use dynamic WEP from being authenticated, do not enable the WEP40 or WEP104 cipher suite in the service profile.

To allow a client that uses static WEP to be authenticated, configure the same WEP keys on the client and the service profile.

Table 6 lists the encryption support for WPA and non-WPA clients.

Table 6: Encryption Support for WPA and Non-WPA Clients

WSS Software Encryption Type	Client Encryption Type					
	WPA—CCMP	**WPA—TKIP**	**WPA—WEP40**	**WPA—WEP104**	**Dynamic WEP**	**Static WEP**
WPA—CCMP	Supported					
WPA—TKIP		Supported				
WPA—WEP40			Supported		Supported	
WPA—WEP104				Supported	Supported	
Dynamic WEP					Supported	
Static WEP						Supported

Configuring WPA

To configure AP access point radios to support WPA:

1. Create a service profile for each SSID that will support WPA clients.
2. Enable the WPA IE in the service profile.
3. Enable the cipher suites you want to support in the service profile. (TKIP is enabled by default.) Optionally, you also can change the countermeasures timer value for TKIP.
4. Map the service profile to the radio profile that will control IEEE settings for the radios.
5. Assign the radio profile to the radios and enable the radios.

If you plan to use PSK authentication, you also need to enable this authentication method and enter an ASCII passphrase or a hexadecimal (raw) key.

Creating a Service Profile for WPA

Encryption parameters apply to all users who use the SSID configured by a service profile. To create a service profile, use the following command:

set service-profile *name*

To create a new service profile named *wpa*, type the following command:

```
23x0# set service-profile wpa
success: change accepted.
```

Enabling WPA

To enable WPA, you must enable the WPA information element (IE) in the service profile. To enable the WPA IE, use the following command:

set service-profile *name* **wpa-ie {enable | disable}**

To enable WPA in service profile *wpa*, type the following command:

```
23x0# set service-profile wpa wpa-ie enable
success: change accepted.
```

Specifying the WPA Cipher Suites

To use WPA, at least one cipher suite must be enabled. You can enable one or more of the following cipher suites:

- CCMP
- TKIP
- 40-bit WEP
- 104-bit WEP

By default, TKIP is enabled and the other cipher suites are disabled.

To enable or disable cipher suites, use the following commands:

set service-profile *name* **cipher-ccmp {enable | disable}**

set service-profile *name* **cipher-tkip {enable | disable}**

set service-profile *name* **cipher-wep104 {enable | disable}**

set service-profile *name* **cipher-wep40 {enable | disable}**

To enable the 40-bit WEP cipher suite in service profile *wpa*, type the following command:

```
23x0# set service-profile wpa cipher-wep40 enable
success: change accepted.
```

After you type this command, the service profile supports TKIP and 40-bit WEP.



Caution! AES (CCMP) encryption is not supported on models AP-101 and AP-122. Do not attempt to enable CCMP in a service profile that is mapped to a radio profile that contains AP model AP-101 or AP-122. Otherwise, the WSS switch's configuration file can be lost the next time the software is restarted. If your network contains model AP-101 or AP-122 APs, create a separate service profile for the other AP models that will run CCMP and enable CCMP only in that profile.



Note. Microsoft Windows XP does not support WEP with WPA. To configure a service profile to provide WEP for XP clients, leave WPA disabled and see "Configuring WEP" on page 209.

Changing the TKIP Countermeasures Timer Value

By default, WSS Software enforces TKIP countermeasures for 60,000 ms (60 seconds) after a second MIC failure within a one-minute interval. To change the countermeasures timer value, use the following command:

set service-profile *name* **tkip-mc-time** *wait-time*

To change the countermeasures wait time in service profile *wpa* to 30 seconds, type the following command:

```
23x0# set service-profile wpa tkip-mc-time 30000
success: change accepted.
```

Enabling PSK Authentication

By default, WPA uses 802.1X dynamic keying. If you plan to use static keys, you must enable PSK authentication and configure a passphrase or the raw key. You can configure the passphrase or key globally. You also can configure keys on an individual MAC client basis.

By default, 802.1X authentication remains enabled when you enable PSK authentication.

To enable PSK authentication, use the following command:

set service-profile *name* **auth-psk {enable | disable}**

To enable PSK authentication in service profile *wpa*, type the following command:

```
23x0# set service-profile wpa auth-psk enable
success: change accepted.
```

Configuring a Global PSK Passphrase or Raw Key for All Clients

To configure a global passphrase for all WPA clients, use the following command:

set service-profile *name* **psk-phrase** *passphrase*

The passphrase must be exactly 63 characters long, including blanks. If you use blanks, you must enclose the string in quotation marks.

To configure service profile *wpa* to use passphrase *1234567890123<>?=+&% The quick brown fox jumps over the lazy sl*, type the following command:

```
23x0# set service-profile wpa psk-phrase "1234567890123<>?=+&% The quick brown
   fox jumps over the lazy sl"
success: change accepted.
```

As an alternative to entering a passphrase, which WSS Software converts into a key, you can enter the key itself in raw hexadecimal format. To enter a PSK key in raw format, use the following command:

set service-profile *name* **psk-raw** *hex*

For *hex*, type a 64-bit ASCII string representing a 32-digit hexadecimal number. Enter the two-character ASCII form of each hexadecimal number.

Examples To configure service profile *wpa* to use a raw PSK with PSK clients, type a command such as the following:

```
23x0# set service-profile wpa psk-raw
   c25d3fe4483e867d1df96eaacdf8b02451fa0836162e758100f5f6b87965e59d
success: change accepted.
```

Disabling 802.1X Authentication for WPA

To disable 802.1X authentication for WPA clients, use the following command:

set service-profile *name* **auth-dot1x {enable | disable}**



Note. This command does not disable 802.1X authentication for non-WPA clients.

To disable WPA authentication in service profile *wpa*, type the following command:

```
23x0# set service-profile wpa auth-dot1x disable
success: change accepted.
```

Displaying WPA Settings

To display the WPA settings in a service profile, use the following command:

show service-profile {*name* | **?**}

To display the WPA settings in effect in service profile *wpa*, type the following command:

```
23x0# show service-profile wpa
ssid-name:          private    ssid-type:           crypto
beacon:                yes    auth-fallthru: last-resort
WEP Key 1 value:    <none>    WEP Key 2 value:    <none>
WEP Key 3 value:    <none>    WEP Key 4 value:    <none>
WEP Unicast Index:       1    WEP Multicast Index:     1
Shared Key Auth:        NO
WPA enabled:
    ciphers: cipher-tkip, cipher-wep40
    authentication: 802.1X
    TKIP countermeasures time: 30000ms
```

The WPA settings appear at the bottom of the output.

Note. The WPA fields appear in the **show service-profile** output only when WPA is enabled.

Assigning the Service Profile to Radios and Enabling the Radios

After you configure WPA settings in a service profile, you can map the service profile to a radio profile, assign the radio profile to radios, and enable the radios to activate the settings.

To map a service profile to a radio profile, use the following command:

set radio-profile *name* **service-profile** *name*

To assign a radio profile to radios and enable the radios, use the following command:

set ap *port-list* **radio** {**1** | **2**} **radio-profile** *name* **mode** {**enable** | **disable**}

To map service profile *wpa* to radio profile *bldg1*, type the following command:

```
23x0# set radio-profile blgd1 service-profile wpa
success: change accepted.
```

To assign radio profile *bldg1* to radio 1 on ports 5-8, 11-14, and 16 and enable the radios, type the following command:

```
23x0# set ap 5-8,11-14,16 radio 1 radio-profile bldg1 mode enable
success: change accepted.
```

To assign radio profile *bldg1* to radio 2 on ports 11-14 and port 16 and enable the radios, type the following command:

```
23x0# set ap 11-14,16 radio 2 radio-profile bldg1 mode enable
success: change accepted.
```

Configuring RSN (802.11i)

Robust Security Network (RSN) provides 802.11i support. RSN uses AES encryption. You can configure a service profile to support RSN clients exclusively, or to support RSN with WPA clients, or even RSN, WPA and WEP clients.

The configuration tasks for a service profile to use RSN are similar to the tasks for WPA:

1. Create a service profile for each SSID that will support RSN clients.
2. Enable the RSN IE in the service profile.
3. Enable the cipher suites you want to support in the service profile. (TKIP is enabled by default.) Optionally, you also can change the countermeasures timer value for TKIP.
4. Map the service profile to the radio profile that will control IEEE settings for the radios.
5. Assign the radio profile to the radios and enable the radios.

If you plan to use PSK authentication, you also need to enable this authentication method and enter an ASCII passphrase or a hexadecimal (raw) key.

Creating a Service Profile for RSN

Encryption parameters apply to all users who use the SSID configured by a service profile. To create a service profile, use the following command:

set service-profile *name*

To create a new service profile named *rsn*, type the following command:

```
23x0# set service-profile rsn
success: change accepted.
```

Enabling RSN

To enable RSN, you must enable the RSN information element (IE) in the service profile. To enable the RSN IE, use the following command:

set service-profile *name* **rsn-ie {enable | disable}**

To enable RSN in service profile *wpa*, type the following command:

```
23x0# set service-profile rsn rsn-ie enable
success: change accepted.
```

Specifying the RSN Cipher Suites

To use RSN, at least one cipher suite must be enabled. You can enable one or more of the following cipher suites:

- CCMP
- TKIP
- 40-bit WEP
- 104-bit WEP

By default, TKIP is enabled and the other cipher suites are disabled.

To enable or disable cipher suites, use the following commands:

set service-profile *name* **cipher-ccmp** {**enable** | **disable**}

set service-profile *name* **cipher-tkip** {**enable** | **disable**}

set service-profile *name* **cipher-wep104** {**enable** | **disable**}

set service-profile *name* **cipher-wep40** {**enable** | **disable**}

To enable the CCMP cipher suite in service profile *rsn*, type the following command:

```
23x0# set service-profile rsn cipher-ccmp enable
success: change accepted.
```

After you type this command, the service profile supports both TKIP and CCMP.



Caution! AES (CCMP) encryption is not supported on models MP-101 and MP-122. Do not attempt to enable CCMP in a service profile that is mapped to a radio profile that contains AP model MP-101 or MP-122. Otherwise, the WSS switch's configuration file can be lost the next time the software is restarted. If your network contains model AP-101 or MP-122 APs, create a separate service profile for the other AP models that will run CCMP and enable CCMP only in that profile.



Note. Microsoft Windows XP does not support WEP with RSN. To configure a service profile to provide WEP for XP clients, leave RSN disabled and see "Configuring WEP" on page 209.

Changing the TKIP Countermeasures Timer Value

To change the TKIP countermeasures timer, see "Changing the TKIP Countermeasures Timer Value" on page 204. The procedure is the same for WPA and RSN.

Enabling PSK Authentication

To enable PSK authentication, see "Enabling PSK Authentication" on page 204. The procedure is the same for WPA and RSN.

Displaying RSN Settings

To display the RSN settings in a service profile, use the following command:

show service-profile {*name* | **?**}

The RSN settings appear at the bottom of the output.



Note. The RSN-related fields appear in the **show service-profile** output only when RSN is enabled.

Assigning the Service Profile to Radios and Enabling the Radios

After you configure RSN settings in a service profile, you can map the service profile to a radio profile, assign the radio profile to radios, and enable the radios to activate the settings.

To map a service profile to a radio profile, use the following command:

set radio-profile *name* **service-profile** *name*

To assign a radio profile to radios and enable the radios, use the following command:

set ap *port-list* **radio** {**1** | **2**} **radio-profile** *name* **mode** {**enable** | **disable**}

To map service profile *rsn* to radio profile *bldg2*, type the following command:

```
23x0# set radio-profile blgd2 service-profile rsn
success: change accepted.
```

Configuring WEP

Wired-Equivalent Privacy (WEP) is a security protocol defined in the 802.11 standard. WEP uses the RC4 encryption algorithm to encrypt data.

To provide integrity checking, WEP access ports and clients check the integrity of a frame's cyclic redundancy check (CRC), generate an integrity check value (ICV), and append the value to the frame before sending it. The radio or client that receives the frame recalculates the ICV and compares the result to the ICV in the frame. If the values match, the frame is processed. If the values do not match, the frame is discarded.

WEP is either dynamic or static depending on how the encryption keys are generated. AP access ports support dynamic WEP and static WEP.

- For dynamic WEP, WSS Software dynamically generates keys for broadcast, multicast, and unicast traffic. WSS Software generates unique unicast keys for each client session and periodically regenerates (rotates) the broadcast and multicast keys for all clients. You can change or disable the broadcast or multicast rekeying interval.
- For static WEP, WSS Software uses statically configured keys typed in the WSS switch's configuration and on the wireless client and does not rotate the keys.

Dynamic WEP encryption is enabled by default. You can disable dynamic WEP support by enabling WPA and leaving the WEP-40 or WEP-104 cipher suites disabled. If you use dynamic WEP, 802.1X must also be configured on the client in addition to WEP.

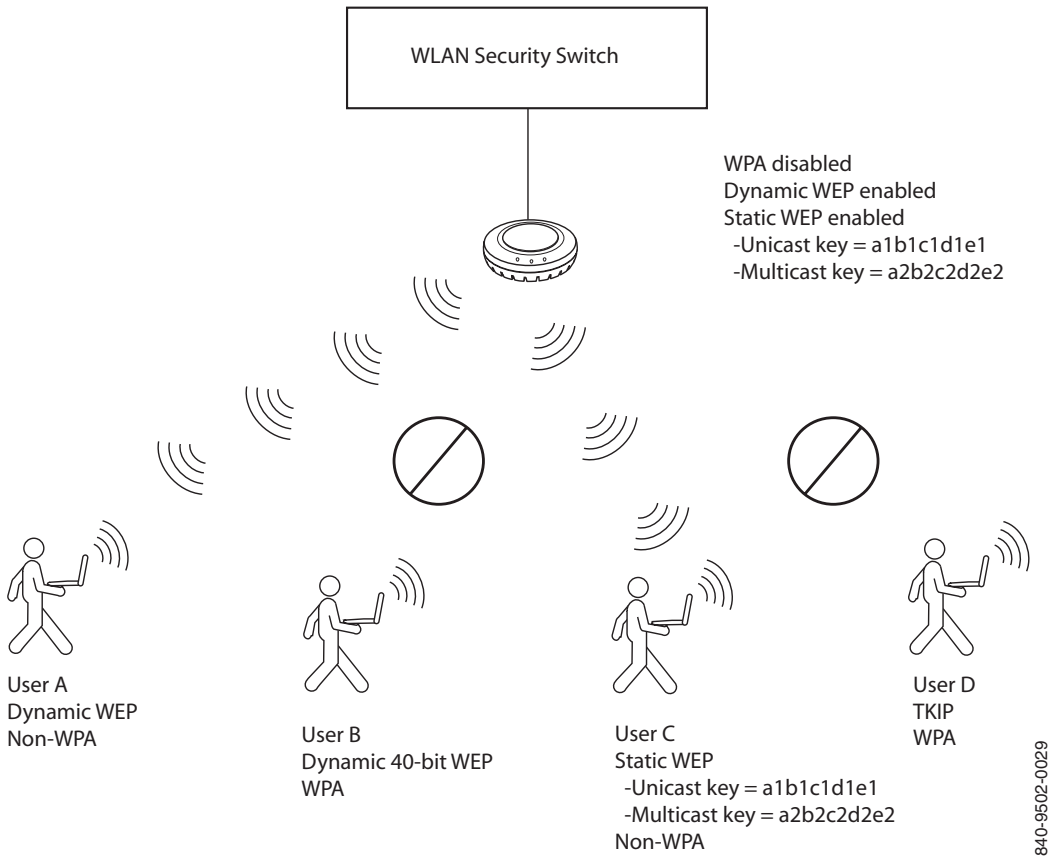
Static WEP encryption is disabled by default. To enable static WEP encryption, configure the static WEP keys and assign them to unicast and multicast traffic. Make sure you configure the same static keys on the clients.

To support dynamic WEP in a WPA environment, enable WPA and enable the WEP-40 or WEP-104 cipher suite. (See "Configuring WPA" on page 203.)

This section describes how to configure and assign static WEP keys. (To change other key-related settings, see "Managing 802.1X Encryption Keys" on page 491.)

Figure 5 shows an example of a radio configured to provide static and dynamic WEP encryption for non-WPA clients. The radio uses dynamically generated keys to encrypt traffic for dynamic WEP clients. The radio also encrypts traffic for static WEP clients whose keys match the keys configured on the radio.

Figure 5. Encryption for Dynamic and Static WEP



Setting Static WEP Key Values

WSS Software supports dynamic WEP automatically. To enable static WEP, configure WEP keys and assign them to unicast and multicast traffic. You can set the values of the four static WEP keys, then specify which of the keys to use for encrypting multicast frames and unicast frames. If you do this, WSS Software continues to support dynamic WEP in addition to static WEP.



Note. If you plan to use static WEP, do not map more than 8 service profiles that contain static WEP keys to the same radio profile.

To set the value of a WEP key, use the following command:

set service-profile *name* **wep key-index** *num* **key** *value*

The **key-index** *num* parameter specifies the index you are configuring. You can specify a value from 1 through 4.

The **key** *value* parameter specifies the hexadecimal value of the key. Type a 10-character ASCII string (representing a 5-digit hexadecimal number) or type a 26-character ASCII string (representing a 13-digit hexadecimal number). You can use numbers or letters. ASCII characters in the following ranges are supported:

- 0 to 9
- A to F
- a to f

To configure WEP key index 1 for radio profile *rp1* to *aabbccddee*, type the following command:

```
23x0# set service-profile rp1 wep key-index 1 key aabbccddee
success: change accepted.
```

Assigning Static WEP Keys

When static WEP is enabled, static WEP key 1 is assigned to unicast and multicast traffic by default. To assign another key to unicast or multicast traffic, use the following commands:

set service-profile *name* **wep active-multicast-index** *num*

set service-profile *name* **wep active-unicast-index** *num*

The *num* parameter specifies the key and the value can be from 1 to 4.

To configure an SSID that uses service profile *wepsrvc* to use WEP key index 2 for encrypting multicast traffic, type the following command:

```
23x0# set service-profile wepsrvc wep active-multicast-index 2
success: change accepted.
```

To configure an SSID that uses service profile *wepsrvc*4 to use WEP key index 4 for encrypting unicast traffic, type the following command:

```
23x0# set service-profile wepsrvc4 wep active-unicast-index 4
success: change accepted.
```

Encryption Configuration Scenarios

The following scenarios provide examples of ways in which you can configure encryption for network clients:

- "Enabling WPA with TKIP" on page 213
- "Enabling Dynamic WEP in a WPA Network" on page 215
- "Configuring Encryption for MAC Clients" on page 217

Enabling WPA with TKIP

The following example shows how to configure WSS Software to provide authentication and TKIP encryption for 801.X WPA clients. This example assumes that pass-through authentication is used for all users. A RADIUS server group performs all authentication and authorization for the users.

1. Create an authentication rule that sends all 802.1X users of SSID *mycorp* in the *EXAMPLE* domain to the server group *shorebirds* for authentication. Type the following command:

   23x0# **set authentication dot1x ssid mycorp EXAMPLE* pass-through shorebirds**

2. Create a service profile named *wpa* for the SSID. Type the following command:

   23x0# **set service-profile wpa**
   ```
   success: change accepted.
   ```

3. Set the SSID in the service profile to *mycorp*. Type the following command:

   23x0# **set service-profile wpa ssid-name wpa**
   ```
   success: change accepted.
   ```

4. Enable WPA in service profile *wpa*. Type the following command:

   23x0# **set service-profile wpa wpa-ie enable**
   ```
   success: change accepted.
   ```

   TKIP is already enabled by default when WPA is enabled.

5. Display the service profile *wpa* to verify the changes. Type the following command:

   23x0# **show service-profile wpa**
   ```
   ssid-name:         mycorp     ssid-type:          crypto
   beacon:                 yes    auth-fallthru: last-resort
   WEP Key 1 value:    <none>    WEP Key 2 value:    <none>
   WEP Key 3 value:    <none>    WEP Key 4 value:    <none>
   WEP Unicast Index:       1    WEP Multicast Index:     1
   Shared Key Auth:        NO
   WPA enabled:
       ciphers: cipher-tkip
       authentication: 802.1X
       TKIP countermeasures time: 60000ms
   ```

6. Map service profile *wpa* to radio profile *rp1*. Type the following commands:

   23x0# **set radio-profile rp1 service-profile wpa**
   ```
   success: change accepted.
   ```

7. Apply radio profile *rp1* to radio 1 on port 5 and to radios 1 and 2 on port 11, enable the radios, and verify the configuration changes. Type the following commands:

   23x0# **set ap 5,11 radio 1 radio-profile rp1 mode enable**
   ```
   success: change accepted.
   ```

   23x0# **set ap 11 radio 2 radio-profile rp1 mode enable**
   ```
   success: change accepted.
   ```

```
23x0# show ap config
Port  5: AP model: AP-241, POE:  enable, bias: high, name: AP05
           boot-download-enable: YES
           load balancing group: none
  Radio 1: type: 802.11a, mode:  enabled, channel: 36
  tx pwr:  1, profile: rp1
  auto-tune max-power: default, min-client-rate: 5.5, max-retransmissions: 10
Port  11: AP model: AP-252, POE:  enable, bias: high, name: AP11
           boot-download-enable: YES
           load balancing group: none
  Radio 1: type: 802.11g, mode:  enabled, channel: 6
  tx pwr:  1, profile: rp1
  auto-tune max-power: default, min-client-rate: 5.5, max-retransmissions: 10
  Radio 2: type: 802.11a, mode: enabled, channel: 36
  tx pwr:  1, profile: rp1
  auto-tune max-power: default, min-client-rate: 24, max-retransmissions: 10
```

8 Save the configuration. Type the following command:

```
23x0# save config
success: configuration saved.
```

Enabling Dynamic WEP in a WPA Network

The following example shows how to configure WSS Software to provide authentication and encryption for 801.X dynamic WEP clients, and for 801.X WPA clients using TKIP. This example assumes that pass-through authentication is used for all users. The commands are the same as those in "Enabling WPA with TKIP" on page 213, with the addition of a command to enable a WEP cipher suite. The WEP cipher suite allows authentication and encryption for both WPA and non-WPA clients that want to authenticate using dynamic WEP.

1. Create an authentication rule that sends all 802.1X users of SSID *mycorp* in the *EXAMPLE* domain to the server group *shorebirds* for authentication. Type the following command:

   23x0# **set authentication dot1x ssid thiscorp EXAMPLE* pass-through shorebirds**

2. Create a service profile named *wpa-wep* for the SSID. Type the following command:

   23x0# **set service-profile wpa-wep**
   success: change accepted.

3. Set the SSID in the service profile to *thiscorp*. Type the following command:

   23x0# **set service-profile wpa-wep ssid-name thiscorp**
   success: change accepted.

4. Enable WPA in service profile *wpa-wep*. Type the following command:

   23x0# **set service-profile wpa-wep wpa-ie enable**
   success: change accepted.

5. Enable the WEP40 cipher suite in service profile *wpa-wep*. Type the following command:

   23x0# **set service-profile wpa-wep cipher-wep40 enable**
   success: change accepted.

   TKIP is already enabled by default when WPA is enabled.

6. Display the service profile *wpa-wep* to verify the changes. Type the following command:

   23x0# **show service-profile wpa-wep**
   ```
   ssid-name:          mycorp     ssid-type:          crypto
   beacon:                yes     auth-fallthru: last-resort
   WEP Key 1 value:    <none>     WEP Key 2 value:    <none>
   WEP Key 3 value:    <none>     WEP Key 4 value:    <none>
   WEP Unicast Index:       1     WEP Multicast Index:     1
   Long Preamble:         YES     Shared Key Auth:        NO
   WPA enabled:
       ciphers: cipher-tkip, cipher-wep40
       authentication: 802.1X
       TKIP countermeasures time: 60000ms
   ```

7. Map service profile *wpa-wep* to radio profile *rp2*. Type the following commands:

   23x0# **set radio-profile rp2 service-profile wpa-wep**
   success: change accepted.

8. Apply radio profile *rp2* to radio 1 on port 5 and to radios 1 and 2 on port 11, enable the radios, and verify the configuration changes. Type the following commands:

   23x0# **set ap 5,11 radio 1 radio-profile rp2 mode enable**

```
success: change accepted.
```

23x0# **set ap 11 radio 2 radio-profile rp2 mode enable**

```
success: change accepted.
```

23x0# **show ap config**

```
Port  5: AP model: AP-241, POE:  enable, bias: high, name: AP05
boot-download-enable: YES
           load balancing group: none
  Radio 1: type: 802.11a, mode:  enabled, channel: 36
  tx pwr:  1, profile: rp2
  auto-tune max-power: default, min-client-rate: 5.5, max-retransmissions: 10
Port  11: AP model: AP-252, POE:  enable, bias: high, name: AP11
           boot-download-enable: YES
           load balancing group: none
  Radio 1: type: 802.11g, mode:  enabled, channel: 6
  tx pwr:  1, profile: rp2
  auto-tune max-power: default, min-client-rate: 5.5, max-retransmissions: 10
  Radio 2: type: 802.11a, mode: enabled, channel: 36
  tx pwr:  1, profile: rp2
  auto-tune max-power: default, min-client-rate: 24, max-retransmissions: 10
```

9 Save the configuration. Type the following command:

23x0# **save config**

```
success: configuration saved.
```

Configuring Encryption for MAC Clients

The following example shows how to configure WSS Software to provide PSK authentication and TKIP or 40-bit WEP encryption for MAC clients:

1. Create an authentication rule that sends all MAC users of SSID *voice* to the local database for authentication and authorization. Type the following command:

   ```
   23x0# set authentication mac ssid voice * local
   success: configuration saved.
   ```

2. Configure a MAC user group named *wpa-for-mac* that assigns all MAC users in the group to VLAN *blue*. Type the following command:

   ```
   23x0# set mac-usergroup wpa-for-mac attr vlan-name blue
   success: configuration saved.
   ```

3. Add MAC users to MAC user group *wpa-for-mac*. Type the following commands:

   ```
   23x0# set mac-user aa:bb:cc:dd:ee:ff group wpa-for-mac
   success: configuration saved.

   23x0# set mac-user a1:b1:c1:d1:e1:f1 group wpa-for-mac
   success: configuration saved.
   ```

4. Verify the AAA configuration changes. Type the following command:

   ```
   23x0# show aaa
   Default Values
   authport=1812 acctport=1813 timeout=5 acct-timeout=5
   retrans=3 deadtime=0 key=(null) author-pass=(null)

   Radius Servers
   Server                  Addr           Ports   T/o Tries Dead
   State
   ------------------------------------------------------------------
   ----

   Server groups

   set authentication mac ssid voice * local

   mac-usergroup wpa-for-mac
      vlan-name = blue

   mac-user aa:bb:cc:dd:ee:ff
      Group = wpa-for-mac

   mac-user a1:b1:c1:d1:e1:f1
      Group = wpa-for-mac
   ```

5. Create a service profile named *wpa-wep-for-mac* for SSID voice. Type the following command:

   ```
   23x0# set service-profile wpa-wep-for-mac
   ```

```
success: change accepted.
```

6 Set the SSID in the service profile to *voice*. Type the following command:

```
23x0# set service-profile wpa-wep-for-mac ssid-name voice
success: change accepted.
```

7 Enable WPA in service profile *wpa-wep-for-mac*. Type the following command:

```
23x0# set service-profile wpa-wep-for-mac wpa-ie enable
success: change accepted.
```

8 Enable the WEP40 cipher suite in service profile *wpa-wep-for-mac*. Type the following command:

```
23x0# set service-profile wpa-wep-for-mac cipher-wep40 enable
success: change accepted.
```

TKIP is already enabled by default when WPA is enabled.

9 Enable PSK authentication in service profile *wpa-wep-for-mac*. Type the following command:

```
23x0# set service-profile wpa-wep-for-mac auth-psk enable
success: change accepted.
```

10 Configure a passphrase for the preshared key. Type the following command:

```
23x0# set service-profile wpa-wep-for-mac psk-phrase "passphrase to convert into a
preshared key"
success: change accepted.
```

11 Display the WPA configuration changes. Type the following command:

```
23x0# show service-profile wpa-wep-for-mac
ssid-name:         voice      ssid-type:          crypto
beacon:                yes    auth-fallthru: last-resort
WEP Key 1 value:    <none>    WEP Key 2 value:    <none>
WEP Key 3 value:    <none>    WEP Key 4 value:    <none>
WEP Unicast Index:       1    WEP Multicast Index:     1
Long Preamble:         YES    Shared Key Auth:        NO
WPA enabled:
    ciphers: cipher-tkip, cipher-wep40
    authentication: pre-shared key
    TKIP countermeasures time: 60000ms
    pre-shared-key: 92f99cd49e186cadee13fda7b2a2bac78975
a5723a4a6b31b5b5395d6b001dbe
```

12 Map service profile *wpa-wep-for-mac* to radio profile *rp3*. Type the following commands:

```
23x0# set radio-profile rp3 service-profile wpa-wep-for-mac
success: change accepted.
```

13 Apply radio profile *rp3* to radio 1 on port 4 and to radios 1 and 2 on port 6 and enable the radios, and verify the configuration changes. Type the following commands:

```
23x0# set ap 4,6 radio 1 radio-profile rp3 mode enable
success: change accepted.
```

```
23x0# set ap 6 radio 2 radio-profile rp3 mode enable
```

```
        success: change accepted.
```

23x0# **show ap config**

```
Port  4: AP model: AP-241, POE:  enable, bias: high, name: AP04
           boot-download-enable: YES
           load balancing group: none
  Radio 1: type: 802.11a, mode:  enabled, channel: 36
  tx pwr:  1, profile: rp3
  auto-tune max-power: default, min-client-rate: 5.5, max-retransmissions: 10
Port  6: AP model: MP-252, POE:  enable, bias: high, name: AP06
           boot-download-enable: YES
           load balancing group: none
  Radio 1: type: 802.11g, mode:  enabled, channel: 6
  tx pwr:  1, profile: rp3
  auto-tune max-power: default, min-client-rate: 5.5, max-retransmissions: 10
  Radio 2: type: 802.11a, mode: enabled, channel: 36
  tx pwr:  1, profile: rp3
  auto-tune max-power: default, min-client-rate: 24, max-retransmissions: 10
```

14 Save the configuration. Type the following command:

23x0# **save config**

```
success: configuration saved.
```

Configuring AP access points

AP Overview 221
Configuring AP access points 247
Disabling or Reenabling Radios 277
Displaying AP Information 281

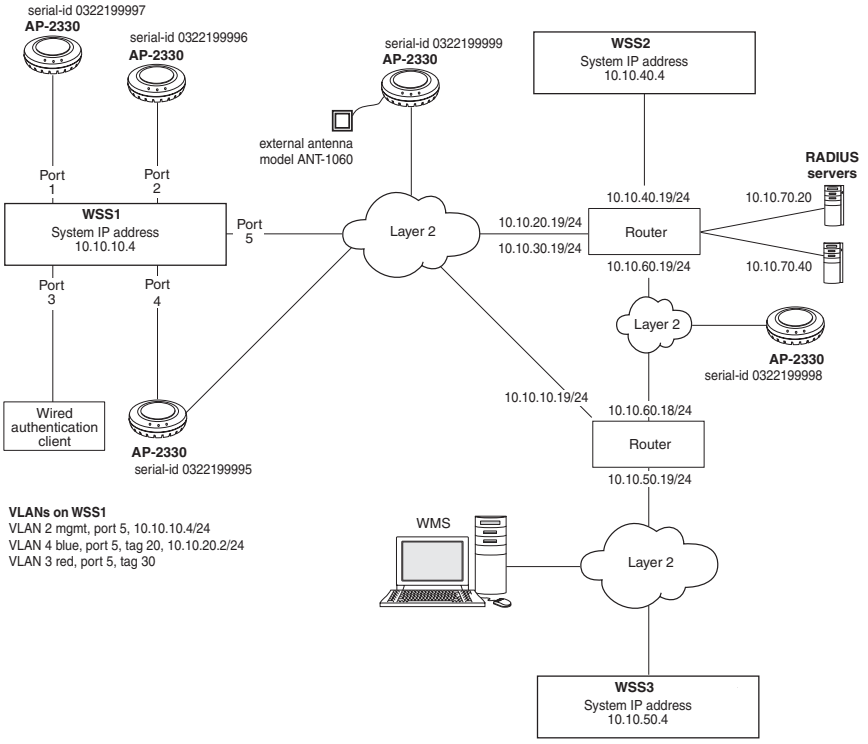
AP contain radios that provide networking between your wired network and IEEE 802.11 wireless users. An AP connects to the wired network through a 10/100 Ethernet link and connects to wireless users through radio signals.

AP Overview

Figure 6 on page 222 shows an example of a Nortel network containing AP access points and WSSs. An AP can be directly connected to a WSS port or indirectly connected to an WSS switch through a Layer 2 or IPv4 Layer 3 network. For redundancy, an AP can have one of the following combinations of multiple connections:

- Two direct connections to a single WSS or two WSSs
- Up to four indirect connections to WSSs through intermediate Layer 2 or Layer 3 networks
- One direct connection to a WSS and up to three indirect connections to WSSs through intermediate Layer 2 or Layer 3 networks

Figure 6. Example Nortel Network



To configure AP access ports, perform the following tasks, in this order:

- Specify the country of operation.
- Configure AP access ports, Distributed AP connections, and dual homing.
- If required, configure radio-specific parameters, which include the channel number, transmit power, and external antenna model.

Note. You do not need to set channels and power if you use RF Auto-Tuning to set these values. You do not need to specify an external antenna model unless a radio uses an external antenna.

- Configure SSID and encryption settings in a service profile.
- Map the service profile to a radio profile, assign the radio profile to radios, and enable the radios.

Country of Operation

Before you can configure AP access ports and radio parameters, you must specify the country in which you plan to operate the radios. Since each country has different regulatory environments, the country code determines the transmit power levels and channels you can configure on the radios. WSS Software ensures that the values you can configure are valid for the country you specify.

Directly Connected APs and Distributed APs

To configure the WSS to support an AP access port, you must first determine how the AP will connect to the switch. There are two types of AP to WSS connection: direct and distributed.

- In direct connection, an AP connects to one or two 10/100 ports on a WSS. The WSS port is then configured specifically for a direct attachment to an AP. There is no intermediate networking equipment between the WSS and AP and only one AP is connected to the WSS port. The WSS 10/100 port provides PoE to the AP. The WSS also forwards data only to and from the configured AP on that port. The port numbers on the WSS configured for directly attached APs reference a particular AP.
- An AP that is not directly connected to a WSS is considered a Distributed AP. There may be intermediate Layer 2 switches or Layer 3 IP routers between the WSS and AP. The WSS may communicate to the Distributed AP through any network port. (A network port is any port connecting the switch to other networking devices, such as switches and routers, and it can also be configured for 802.1Q VLAN tagging.) The WSS contains a configuration for a Distributed AP based on the AP's serial number. Similar to ports configured for directly connected APs, Distributed AP configurations are numbered and can reference a particular AP. These numbered configurations do not, however, reference any physical port.

Distributed AP Network Requirements

Because Distributed APs are not directly attached to a WSS, they require additional support from the network in order to function. Information on the booting and operation sequence for Distributed APs is covered in the section "AP Boot Process" on page 231.

- Power—PoE must be provided on one of the Ethernet connections to the AP. Be sure to use a PoE injection device that has been tested by Nortel. (Contact Nortel for information.) Providing PoE on both of the Ethernet connections (on models that have two Ethernet ports) allows redundant PoE.
- DHCP—A Distributed AP uses TCP/IP for communication, and relies on DHCP to obtain IP parameters. Therefore, DHCP services must be available on the subnet that the AP is connected to. DHCP must provide the following parameters to the AP:
    - IP address
    - Domain name
    - DNS server address
    - Gateway address
- DNS—If the intermediate network between the WSS and Distributed AP includes one or more IP routers, create a NORTEL.*mynetwork*.com or wlan-switch.*mynetwork*.com entry on the DNS server. The entry needs to map one of these names to the system IP address of the switch. If the subnet contains more than one WSS in the same Mobility Domain, you can use the system IP address of any of the switches. (For redundancy, you can create more than one DNS entry, and map each entry to a different WSS in the subnet.)

    The DNS entry allows the AP to communicate with a WSS that is not on the AP's subnet. If the AP is unable to locate a WSS on the subnet it is connected to, the AP sends DNS requests to both *NORTEL* and *wlan-switch*, where the DNS suffix for *mynetwork*.com is learned through DHCP.

    - If only *NORTEL* is defined in DNS, the AP contacts the WSS whose IP address is returned for *NORTEL*.

- If only *wlan-switch* is defined in DNS, the AP contacts the WSS whose IP address is returned for *wlan-switch*.
- If both *NORTEL* and *wlan-switch* are defined in DNS, the AP contacts the WSS whose IP address is returned for *NORTEL*. The AP ignores the IP address returned for *wlan-switch*.
- If both *NORTEL* and *wlan-switch* are defined in DNS, and the AP is unable to contact the IP address returned for *NORTEL*, the AP never contacts the IP address returned for *wlan-switch*. The AP does not boot.

Distributed APs and STP

A Distributed AP is a leaf device. You do not need to enable STP on the port that is directly connected to the AP.

If Spanning Tree Protocol (STP) is enabled on the port that is directly connected to a Distributed AP, you might need to change the STP configuration on the port, to allow the AP to boot.



Note. STP on a port directly connected to a Distributed AP can prevent the AP from booting.

As part of the boot process, an AP disables and reenables the link on the port over which the AP is attempting to boot. If STP is enabled on the device that is directly connected to the port, the link state change can cause the port on the other device to leave the forwarding state and stop forwarding traffic. The port remains unable to forward traffic for the duration of the STP forwarding delay.

An AP waits 30 seconds to receive a reply to its DHCP Discover message, then tries to boot using the other AP port. If the boot attempt fails on the other port also, the AP then reattempts to boot on the first port. The process continues until a boot attempt is successful. If STP prevents the other device's port from forwarding traffic during each boot attempt, the AP repeatedly disables and reenables the link, causing STP to repeatedly stop the other device's port from forwarding traffic. As a result, the boot attempt is never successful.

To allow an AP to boot over a link that has STP enabled, do one of the following on the other device:

- Disable STP on the other device's port.
- Enable the port Fast Port feature, if supported, on the other device's port. (On some vendors' devices, this feature is called *PortFast*.)
- If the other device is running Rapid Spanning Tree or Multiple Spanning Tree, set the port into edge port mode.

Distributed APs and DHCP Option 43

The DHCP option 43 field provides a simple and effective way for APs to find WSS switches across an intermediate Layer 3 network, and is especially useful in networks that are geographically distributed or have a flat domain name space. You can use the DHCP option 43 field to provide a list of WSS IP addresses, without the need to configure DNS servers.

To use DHCP option 43, configure the option to contain a comma-separated list of WSS IP addresses or hostnames, in the following format:

ip:*ip-addr1*,*ip-addr2*,. . .

or

host:*hostname1*,*hostname2*,. . .

You can use an IP address list or a hostname list, but not both. If the list contains both types of values, the AP does not attempt to use the list.

The **ip** and **host** keywords can be in lowercase, uppercase (**IP** or **HOST**), or mixed case (example: **Ip**, **Host**, and so on.) You can use spaces after the colon or commas, but spaces are not supported within IP addresses or hostnames. Leading zeroes are supported in IP addresses. For example, 100.130.001.1 is valid.

Valid characters in hostnames are uppercase and lowercase letters, numbers, periods (**.**), and hyphens (**-**). Other characters are not supported.

If you use the **host** option, you must configure the network's DNS server with address records that map the hostnames in the list to the WSS IP addresses.

After receiving a DHCP Ack containing a valid string for option 43, a Distributed AP sends a unicast message to the each WSS switch in the list, to request a software image and configuration. If the AP does not receive a reply to the request after one minute, the AP starts the boot process over with a new DHCP Discover message, this time from AP port 2.

No configuration is required on the WSS itself.

AP Parameters

Table 7 on page 226 summarizes parameters that apply to individual AP access ports, including dual-homing parameters. (For information about parameters for individual radios, see "Configuring a Radio Profile" on page 267 and "Configuring Radio-Specific Parameters" on page 273.)

Table 7: Global AP Parameters

Parameter	Default Value	Description
name	Based on the port or Distributed AP connection number. For example: • AP01 • DAP01	AP name.
bias	**high**	Setting an AP's bias on a WSS to high causes the switch to be preferred over switches with low bias, for booting and managing the AP. **Note:** Bias applies only to WSSs that are indirectly attached to the AP through an intermediate Layer 2 or Layer 3 network. An AP always attempts to boot on AP port 1 first, and if a WSS is directly attached on AP port 1, the AP boots from it regardless of the bias settings.

Table 7: Global AP Parameters (continued)

Parameter	Default Value	Description
group	None	Named set of AP access ports. WSS Software load-balances user sessions among the access ports in the group.
upgrade-firmware	**enable**	Automatic upgrade of boot firmware.
blink	**disable**	LED blink mode—blinking LEDs on an AP make the AP visually easy to identify.

Resiliency and Dual-Homing Options for APs

APs can support a wide variety of resiliency options. Redundancy for PoE, for data link connections and for WSS services can be provided to the AP.

- PoE redundancy—On AP models that have two Ethernet ports, you can provide PoE redundancy by connecting both ports to PoE sources. PoE can come from a directly connected WSS or a PoE injector. Dual-homing support for PoE is automatically enabled when you connect both AP Ethernet ports.
- Data link redundancy—You can provide data link redundancy by connecting both Ethernet ports directly to one WSS, two WSS switches, an intermediate Ethernet switch, or a combination of WSS and Ethernet switch. If an intermediate Ethernet connection is used, you also need a Distributed AP configuration on an WSS somewhere in the network. Dual-homing support for data link redundancy is automatically enabled when you connect both AP Ethernet ports.
- WSS redundancy—You can provide redundancy of WSS services by dual-homing the AP to two directly connected WSSs; or by configuring a Distributed AP configuration either on two or more indirectly connected WSSs, or on a combination of a directly connected WSS and one or more indirectly connected WSSs. To provide WSS redundancy on an AP model that has only one AP port, configure a Distributed AP connection on two or more indirectly connected WSSs.

Bias

On a WSS, configurations for APs have a bias (low or high) associated with them. The default is high. A WSS switch with high bias for an AP is preferred over a WSS with low bias for the AP.

If more than one switch has high bias, or the bias for all connections is the same, the switch that has the greatest capacity to add more active APs is preferred. For example, if one switch has 50 active APs while another switch has 60 active APs, and both switches are capable of managing 80 active APs, the new AP uses the switch that has only 50 active APs.

Note. Bias applies only to WSSs that are indirectly attached to the AP through an intermediate Layer 2 or Layer 3 network. An AP always attempts to boot on AP port 1 first, and if a WSS is directly attached on AP port 1, the AP boots from it regardless of the bias settings.

(To set the bias for an AP configuration, see "Changing Bias" on page 260.)

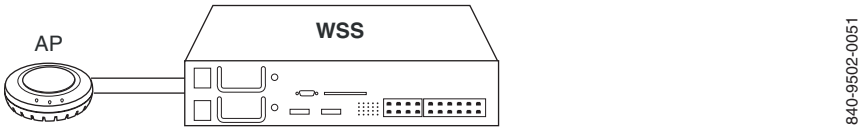
Dual-Homed Configuration Examples

The following sections show examples of dual-homed configurations. You can use any of these configurations to dual home an AP model that has two Ethernet ports. AP models with one Ethernet port support only the dual-homing configuration in "Dual-Homed Distributed Connections to WSSs on One AP Port" on page 231.

Dual-Homed Direct Connections to a Single WSS

Figure 7 shows an example of a dual-homed direct connection to one WSS. In this configuration, if the AP's active data link with the WSS fails, the AP detects the link failure and restarts using the other link on the same switch.

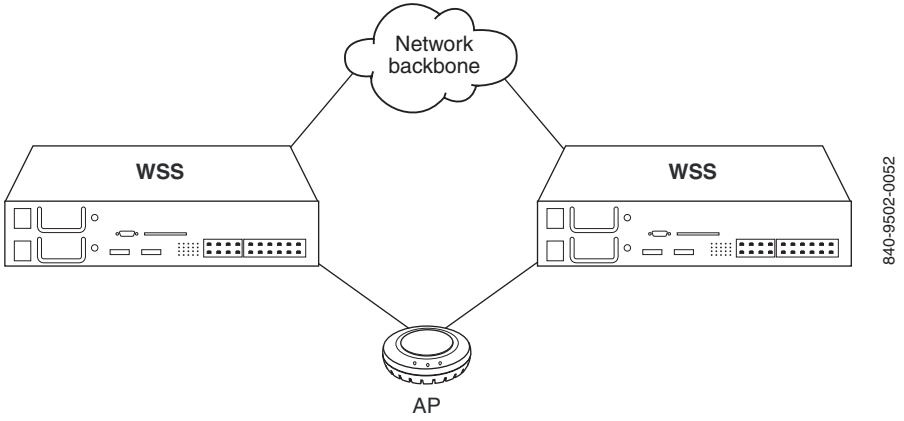
Figure 7. Dual-Homed Direct Connections to a Single WSS



Dual-Homed Direct Connections to Two WSSs

Figure 8 on page 228 shows an example of a dual-homed direct connection to two separate WSS switches. In this configuration, if the active data link fails, the AP access point detects the link failure and restarts using a link to the other switch.

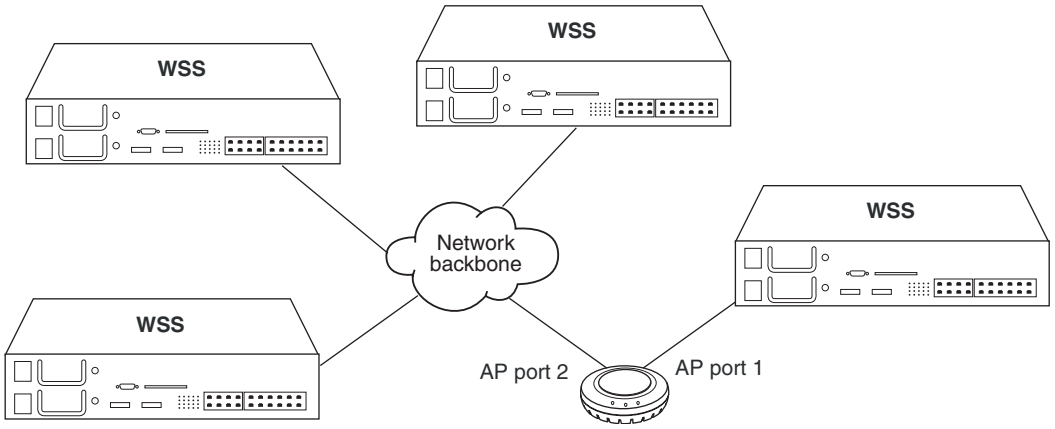
Figure 8. Dual-homed Direct Connections to Two WSSs



Dual-Homed Direct and Distributed Connections to WSSs

Figure 9 shows an example of a dual-homed configuration in which one AP connection is direct and the other is distributed over the network.

Figure 9. Dual-Homed Direct and Distributed Connections to WSSs

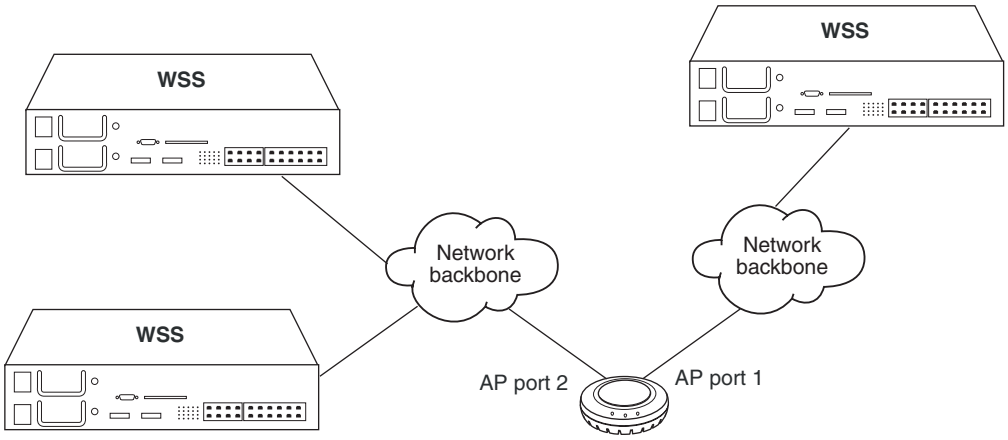


In this example, the AP's port 1 is directly connected to an WSS switch. The AP always attempts to boot first from the directly connected WSS switch. The AP attempts to boot using AP port 2 only if the boot attempt on port 1 fails. If the active data link fails, the WSS reboots using the other link.

Dual-Homed Distributed Connections to WSSs on Both AP Ports

Figure 10 shows an example of a dual-homed configuration in which both AP connections are distributed over the network.

Figure 10. Dual-homed Distributed Connections to WSSs on Both AP Ports

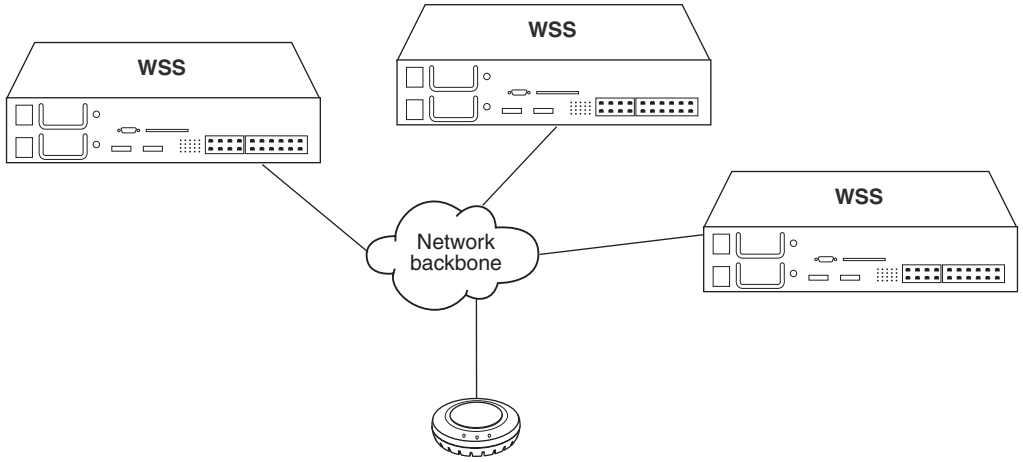


In this configuration, the AP first attempts to boot on its port 1. If more than one WSS has high bias or if all WSSs have the same bias, the AP uses the WSS that has the greatest capacity for new active AP connections.

Dual-Homed Distributed Connections to WSSs on One AP Port

Figure 11 shows an example of an AP with a single physical link to a network containing three WSSs.

Figure 11. Single-homed Connection to Multiple WSSs on One AP Port



In this configuration, the AP sends a boot request on its connected port. WSS switches that are in the same subnet respond to the AP. Switches with high bias for the AP respond immediately, whereas switches with low bias for the AP respond after a brief delay.

If the switches are in another subnet, the AP uses DNS to locate one of the switches, and asks the switch to send the IP address of the best WSS switch to use, based on the bias settings on each switch and the capacity of each switch to add new active AP connections. The AP then requests its image and configuration files from the best WSS switch.

AP Boot Process

An AP access point brings up the link on the AP's port 1 and attempts the boot process outlined below.

If you want the AP to boot from a specific WSS, you must ensure that only one WSS can respond through the AP's port 1 with a high bias under normal operation. If the boot process fails to locate any WSS, the AP then attempts the boot process on the AP's port 2.

Note. The steps below describe the network behavior of a Distributed AP when booting. These steps do not apply to a directly connected AP. The boot process for a directly connected AP occurs strictly between the AP and WSS and makes no use of the network's DHCP or DNS services.

1. The AP sends a DHCP Discover message from the AP's port 1 to the broadcast address.
2. If a DHCP server is present on the subnet or through a router configured to relay DHCP, the server replies with a unicast DHCP Offer message. The Offer message must contain the following parameters:

- IP address for the AP
- Domain name of the network
- IP address of the network's DNS server
- IP address of the subnet's default gateway

Optionally, the Offer message can also contain a list of WSS IP addresses or hostnames, in the option 43 field of the DHCP message.

Continuing the DHCP process, the AP broadcasts a DHCP Request to the DHCP servers, and receives an Ack from a DHCP server. The AP then configures its network connection with the information contained in the Ack message from that server.

3 The AP sends a Find WSS message to UDP port 5000 on the subnet broadcast address.

- WSS switches in the same IP subnet as the AP receive the message and respond with a Find WSS Reply message.
  - If the AP is configured as a Distributed AP on a switch and the connection bias is high, the WSS switch immediately sends a Find WSS Reply message.
  - If the AP is configured as a Distributed AP on a switch but the connection bias is low, that WSS switch waits one second, then sends a Find WSS Reply message. The delay allows switches with high bias for the AP to respond first.
  - If an WSS switch that receives the Find WSS message does not have the Distributed AP in its configuration but another WSS switch in the same Mobility Domain does, the switch waits two seconds, then sends a Find WSS Reply message with the IP address of the best switch to use. The determination of *best* switch is based on the bias settings for the AP on each switch and on the capacity of each switch to add new active AP connections.

  The process skips to step 10.
- If no WSS switches reply, the AP resends the Find WSS broadcast up to 11 more times. If no WSSs reply after all 12 attempts, the AP attempts to find an WSS based on DHCP option 43 values received in the DHCP Ack. The process continues with step 4.

4 This step applies only if the DHCP Ack contained WSS IP addresses or hostnames in the option 43 field. If the Ack did not contain WSS IP addresses or hostnames in the option 43 field, skip to step 5.

If the DHCP Ack message contained a list of WSS IP addresses or hostnames in the DHCP option 43 field, the AP contacts the WSS switches:

- If the DHCP Ack message contained a list of WSS IP addresses, in DHCP option 43, the AP sends a unicast Find WSS message to each address. The process continues with step 8.

- If the DHCP Ack message contained a list of WSS hostnames in DHCP option 43, the AP sends DNS Requests to the DNS server for the IP addresses of the switches, then sends a unicast Find WSS message to each address. The process continues with step 8.

Note. This method requires DNS address records on the DNS server that map the hostnames to the WSS IP addresses.

- If no WSS switches reply, the AP resends the Find WSS messages up to 11 more times. If no WSSs reply after all 12 attempts, the AP tries to find an WSS switch using the DNS server. The process continues with step 5.

5 If the AP is unable to locate an WSS on the subnet it is connected to, and is unable to find an WSS based on DHCP option 43, the AP sends DNS requests to both *NORTEL* and *wlan-switch*, where the DNS suffix for *mynetwork*.com is learned through DHCP.

Note. You must configure a DNS address record on your DNS server for the WSS IP address. Otherwise, the DNS server cannot provide the WSS switch's address to the AP.

6 The DNS server replies with the system IP address of an WSS switch.

- If only *NORTEL* is defined in DNS, the AP sends a unicast Find WSS message to the WSS switch whose IP address is returned for *NORTEL*.
- If only *wlan-switch* is defined in DNS, the AP sends a unicast Find WSS message to the WSS switch whose IP address is returned for *wlan-switch*.
- If both *NORTEL* and *wlan-switch* are defined in DNS, the AP sends a unicast Find WSS message to the WSS switch whose IP address is returned for *NORTEL*. The AP ignores the IP address returned for *wlan-switch*.
- If both *NORTEL* and *wlan-switch* are defined in DNS, and the AP is unable to contact the IP address returned for *NORTEL*, the AP never contacts the IP address returned for *wlan-switch*. The AP does not boot.

7 The AP sends Find WSS requests to the WSS IP addresses given by the DNS reply. If an WSS receives the Find WSS Request, the process continues with step 8.

However, if no WSS switches reply, the AP retries this method up to 11 more times:

- If no WSSs reply after all 12 attempts, the AP begins the process again with step 1 on the other AP port.
- If the other AP port does not have a link or the AP has only one port, the AP instead restarts, and begins the process again with step 1 on the same AP port.

8 The WSS that receives the Find WSS request determines the best WSS for the AP to use, based on the bias settings for the AP on each switch. If more than one switch has high bias for the AP or all switches have the same bias, the WSS suggests the switch that has the highest capacity to add new active AP connections.

9 The WSS sends a unicast Find WSS Reply message to the AP containing the system IP address of the best WSS switch to use.

10 The AP sends a unicast message to the suggested WSS switch, to request a software image and configuration. If the AP does not receive a reply after 10 seconds, the AP reboots and starts the boot process over at step 1.

If an AP does not receive a reply to a DNS request or a request for a system image and configuration after one minute, the AP starts the boot process over with a new DHCP Discover message, this time from AP port 2.

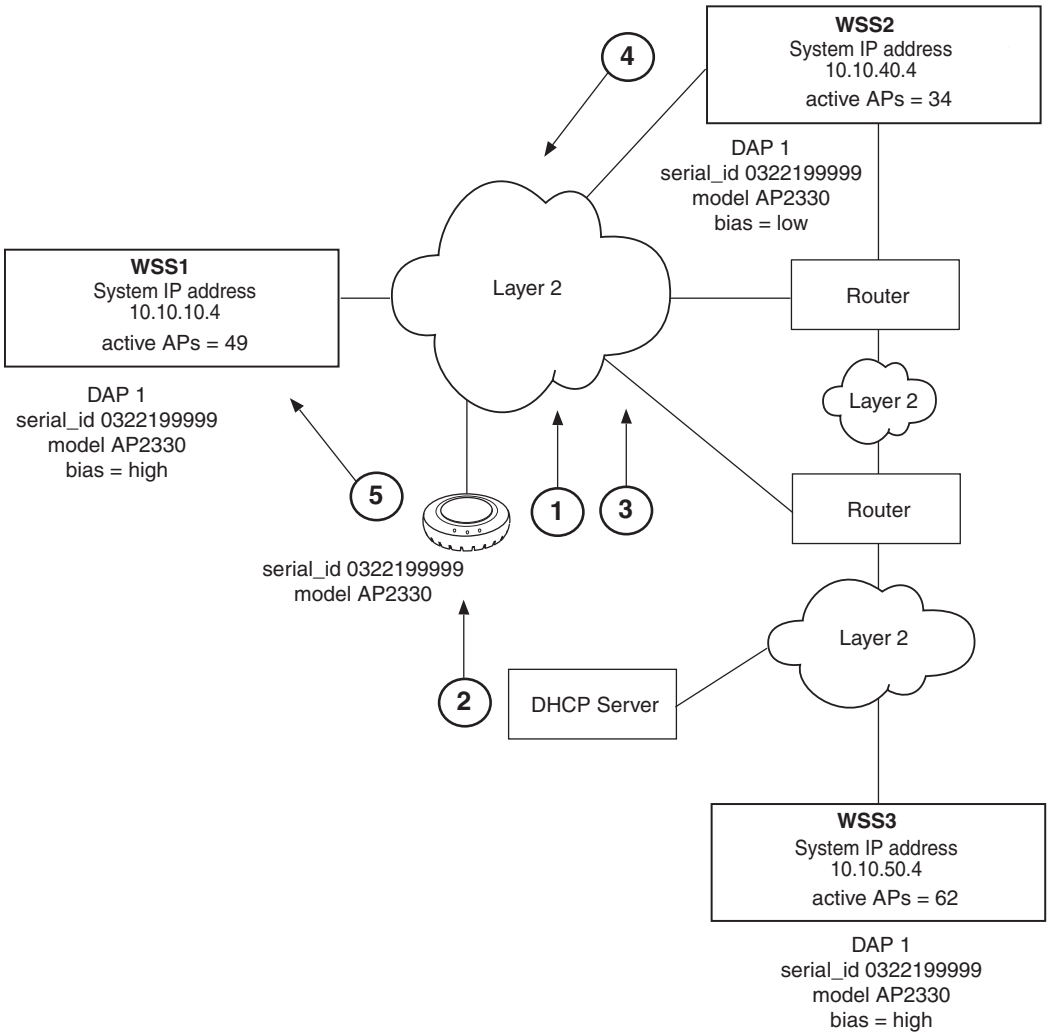
The following figures show AP boot examples:

- Figure 12 on page 235 shows an example of the boot process for an AP connected through a Layer 2 network.
- Figure 13 on page 236 shows an example of the boot process for an AP connected through a Layer 3 network.
- Figure 14 on page 238 shows an example of the boot process for a dual-homed AP that has one direct connection to an WSS switch and an indirect connection through a Layer 2 network.

Example AP Boot over Layer 2 Network

Figure 12 shows an example of the boot process for an AP access point connected through a Layer 2 network. WSS1, WSS2, and WSS3 each have a Distributed AP configuration for the AP.

Figure 12. AP Booting over Layer 2 Network



1 The AP sends a DHCP Discover message from the AP's port 1.

2 DHCP server receives the Discover message (through a relay agent) and replies with a DHCP Offer message containing IP address for the AP, the gateway IP address for the AP's IP subnet, the DNS server address, and the domain name. AP then sends a DHCP Request message to the server and receives an Ack from the server.

3 The AP sends a broadcast Find WSS message to IP subnet broadcast address.

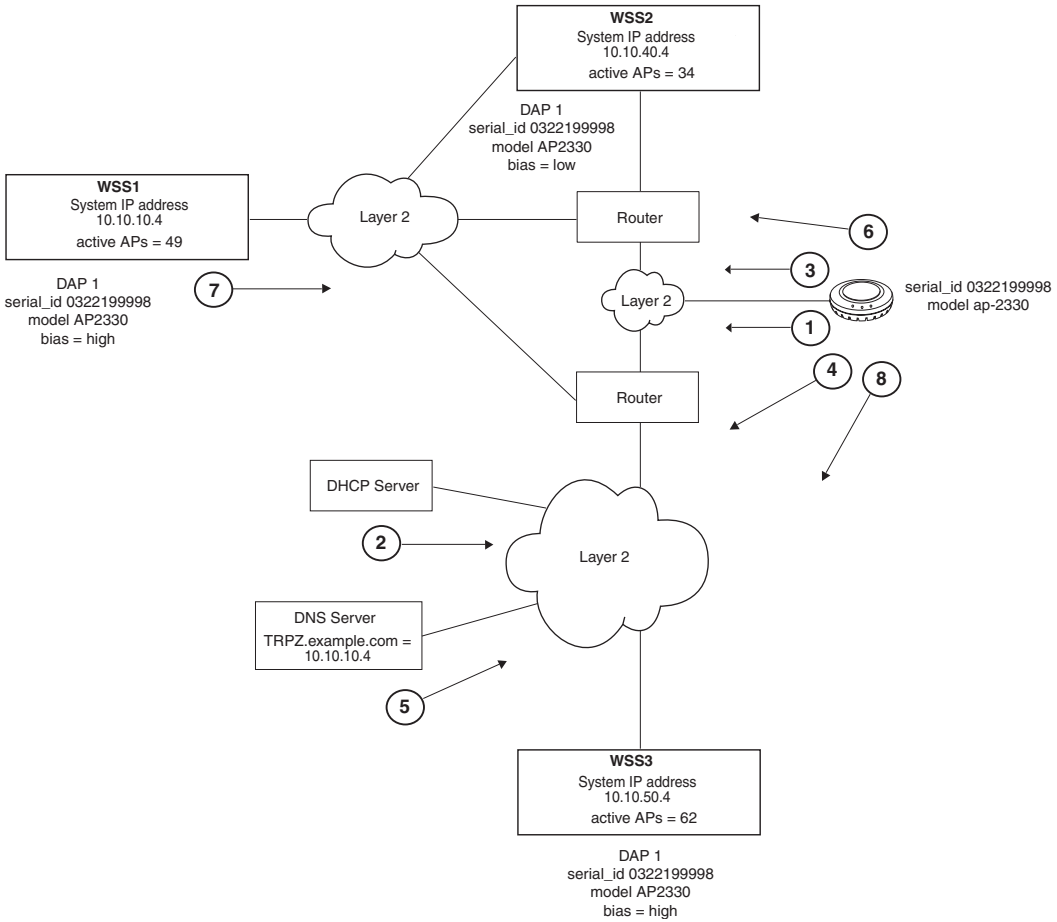
4 WSS1 and WSS3 have high priority for the AP and reply immediately.

5 The AP boots with a software image and configuration from WSS1 because it has fewer active AP connections than WSS3.

Example AP Boot over Layer 3 Network

Figure 13 shows an example of the boot process for an AP connected through a Layer 3 network.

Figure 13. AP Booting over Layer 3 Network



1 The AP sends DHCP Discover message from the AP's port 1.

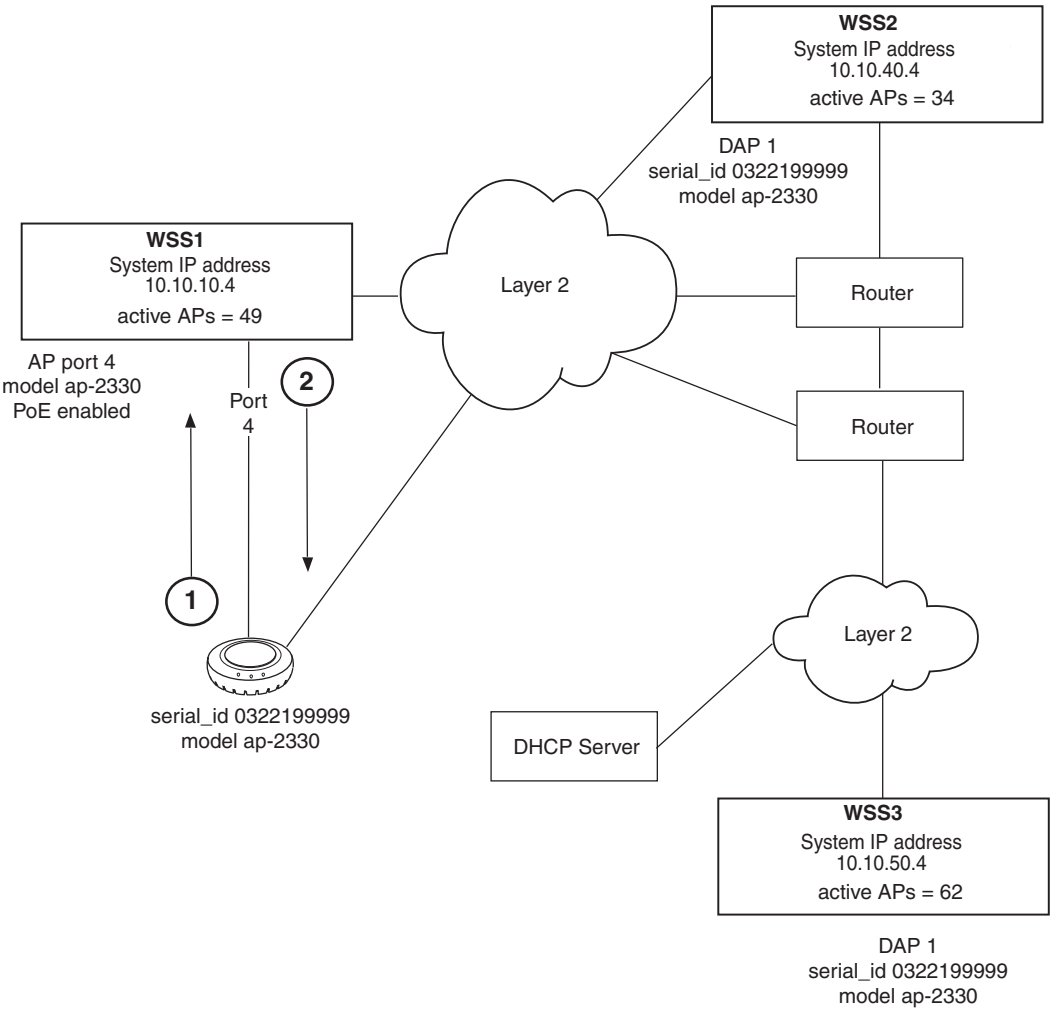
2. The DHCP server replies with a DHCP Offer message containing an IP address for the AP, the gateway IP address for the AP's IP subnet, the DNS server address, and the domain name. AP then sends a DHCP Request message to the server and receives an Ack from the server.
3. The AP sends a broadcast Find WSS message to the IP subnet broadcast address.
4. When no WSS switches reply, the AP resends the Find WSS broadcast 11 more times. After 12 attempts, the AP attempts to find an WSS based on DHCP option 43 values received in the DHCP Ack.
5. When the AP is unable to locate an WSS on the subnet it is connected to, and is unable to find an WSS based on DHCP option 43, the AP then sends a DNS request for *NORTEL.example.com* and *wlan.example.com*.
6. The DNS server sends the system IP address of the WSS switch mapped to *NORTEL.example.com* or *wlan example.com*. In this example, the address is for WSS1.
7. The AP sends a unicast Find WSS message to WSS1.
8. WSS1 receives the Find WSS message and compares the bias settings on each WSS for the AP. More than one WSS has a high bias for the AP, so WSS1 selects the WSS that has the greatest capacity to add new active AP connections. In this example, WSS1 has more capacity. WSS1 sends its own IP address in the Find WSS Reply message to the AP.
9. The AP requests a software image and configuration from WSS1.

Example Boot of Dual-Homed AP

Figure 14 on page 238 shows an example of the boot process for an AP that is dual homed with a direct connection to WSS1 and an indirect connection to WSS2 and WSS3. In this configuration, since the AP is directly connected to an WSS switch, the AP boots using the directly connected WSS switch regardless of the

bias set on any of the WSS switches configured for the AP. Only in the event of a physical port failure would the AP attempt to boot from its port 2.

Figure 14. Dual-Homed AP Booting



1 AP sends a DHCP Discover message from the AP's port 1.

2 Because WSS1 is configured for direct attachment, WSS1 responds *privately* to the AP and provides the AP with its software image and configuration from WSS1. Only in the event of a physical port failure would the AP attempt to boot from its port 2, in which case both WSS1 and WSS2 would respond to the broadcast Find WSS message.

Session Load Balancing

You can assign AP access ports to a load-balancing group. A load-balancing group helps reduce congestion by distributing client sessions among the AP access ports in the group. For example, if an 802.11b/g radio operating on channel 1 is supporting more sessions than a neighboring 802.11b/g radio operating on channel 6, the load-balancing feature can reject association requests to the radio on channel 1.

To balance the sessions, WSS Software rejects an association request for an access port's radio if that radio has at least four more active sessions than the radio of the same type with the least number of active sessions within the group. If the rejected client associates with another access point in the same group, the session load among the access ports in the group becomes more balanced.

Load balancing is based only on association requests for new sessions. Adding an AP access point to a group does not affect sessions that are already active on the access port. In addition, WSS Software does not attempt to rebalance sessions when a client disassociates from an access port. If WSS Software rejects an association request for load-balancing reasons but not for authentication reasons, the rejection does not count as an authentication failure.

Nortel recommends that you configure small groups and ensure that all the radios in the group provide comparable coverage within the same service area.

(To configure a load-balancing group, see "Configuring a Load-Balancing Group" on page 260.)

Service Profiles

A service profile controls advertisement and encryption for an SSID. You can specify the following:

- Whether SSIDs that use the service profile are beaconed
- Whether the SSIDs are encrypted or clear (unencrypted)
- For encrypted SSIDs, the encryption settings to use
- The *fallthru* authentication method for users that are not authenticated with 802.1X or MAC authentication

Table 8 lists the parameters controlled by a service profile and their default values.

Table 8: Defaults for Service Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
auth-dot1x	**enable**	When the Wi-Fi Protected Access (WPA) information element (IE) is enabled, uses 802.1X to authenticate WPA clients.
auth-fallthru	**web-portal**	Uses Web-based AAA for users who do not match an 802.1X or MAC authentication rule for the SSID requested by the user.
auth-psk	**disable**	Does not support using a preshared key (PSK) to authenticate WPA clients.
beacon	**enable**	Sends beacons to advertise the SSID managed by the service profile.
cipher-ccmp	**disable**	Does not use Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) to encrypt traffic sent to WPA clients.
cipher-tkip	**enable**	When the WPA IE is enabled, uses Temporal Key Integrity Protocol (TKIP) to encrypt traffic sent to WPA clients.
cipher-wep104	**disable**	Does not use Wired Equivalent Privacy (WEP) with 104-bit keys to encrypt traffic sent to WPA clients.
cipher-wep40	**disable**	Does not use WEP with 40-bit keys to encrypt traffic sent to WPA clients.
psk-phrase	No passphrase defined	Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients.
psk-raw	No preshared key defined	Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients.

Table 8: Defaults for Service Profile Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
rsn-ie	**disable**	Does not use the RSN IE in transmitted frames.
shared-key-auth	**disable**	Does not use shared-key authentication. This parameter does not enable PSK authentication for WPA. To enable PSK encryption for WPA, use the **set radio-profile auth-psk** command.
ssid-name	**Nortel**	Uses the SSID name *Nortel*.
ssid-type	**crypto**	Encrypts wireless traffic for the SSID.
tkip-mc-time	**60000**	Uses Michael countermeasures for 60,000 ms (60 seconds) following detection of a second MIC failure within 60 seconds.
web-aaa-form	Not configured	For Web-based AAA users, serves the default login web page or, if configured, the SSID-specific login web page.
wep key-index	No keys defined	Uses dynamic WEP rather than static WEP. **Note:** If you configure a WEP key for static WEP, WSS Software continues to also support dynamic WEP.
wep active-multicast-index	**1**	Uses WEP key 1 for static WEP encryption of multicast traffic if WEP encryption is enabled and keys are defined.
wep active-unicast-index	**1**	Uses WEP key 1 for static WEP encryption of unicast traffic if WEP encryption is enabled and keys are defined.
wpa-ie	**disable**	Does not use the WPA IE in transmitted frames.

(To configure a service profile, see "Configuring a Service Profile" on page 265.)

Public and Private SSIDs

Each radio can support the following types of SSIDs:

- Encrypted SSID—Clients using this SSID must use encryption. Use the encrypted SSID for secured access to your enterprise network.

- Clear SSID—Clients using this SSID do not use encryption. Use the clear SSID for public access to nonsecure portions of your network.

All AP access point models except AP-101 and AP-122 can support up to 32 SSIDs per radio. Each SSID can be encrypted or clear, and beaconing can be enabled or disabled on an individual SSID basis.

Each radio has 32 MAC addresses and can therefore support up to 32 SSIDs, with one MAC address assigned to each SSID as its BSSID. An AP access port's MAC address block is listed on a label on the back of the access port. If the AP is already deployed and running on the network, you can display the MAC address assignments by using the **show {ap | dap} status** command.

All MAC addresses on an AP are assigned based on the AP's base MAC address, as described in Table 9 on page 242.

Table 9: MAC Address Allocations on AP access ports

AP access port	**All models**	• The AP has a base MAC address. All the other addresses are assigned based on this address.
Ethernet Ports	**All models**	• Ethernet port 1 equals the AP base MAC address. • Ethernet port 2 (if the AP model has one) equals the AP base MAC address + 1.
Radios and SSIDs	**AP-2330** **AP-233x** **AP-233x** **AP-233x** **AP-233x**	• The 802.11b/g radio equals the AP base MAC address. • The BSSIDs for the SSIDs configured on the 802.11b/g radio end in even numbers. The first BSSID is equal to the AP's base MAC address. The next BSSID is equal to the AP's base MAC address + 2, and so on. • The 802.11a radio equals the AP base MAC address + 1. • The BSSIDs for the SSIDs configured on the 802.11a radio end in odd numbers. The first BSSID is equal to the AP's base MAC address + 1. The next BSSID is equal to the AP's base MAC address + 3, and so on.
	AP-341 **AP-241**	• The radio equals the AP base MAC address. • The BSSIDs for the SSIDs configured on the radio end in even numbers. The first BSSID is equal to the AP's base MAC address. The next BSSID is equal to the AP's base MAC address + 2, and so on.
	AP-122	• The 802.11b radio equals the base MAC address, for both the clear and encrypted SSIDs. • The 802.11a radio equals the base address + 1, for both the clear and encrypted SSIDs.
	AP-101	• The radio equals the base MAC address, for both the clear and encrypted SSIDs.

Models AP-101 and AP-122 are assigned blocks of four MAC addresses each. Each radio on models AP-101 and AP-122 is assigned one MAC address, which is shared by both the clear SSID and the encrypted SSID.

Encryption

Encrypted SSIDs can use the following encryption methods:

- Wi-Fi Protected Access (WPA)
- Non-WPA dynamic Wired Equivalent Privacy (WEP)
- Non-WPA static WEP

Dynamic WEP is enabled by default.

(For more information, including configuration instructions, see "Configuring User Encryption" on page 191.)

Radio Profiles

You can easily assign radio configuration parameters to many radios by configuring a radio profile and assigning the profile to the radios. To use a radio, you must assign a profile to the radio. You can enable the radio when you assign the profile.

Table 10 summarizes the parameters controlled by radio profiles. Generally, the only radio parameters controlled by the profile that you need to modify are the SSIDs and, if applicable, Wi-Fi Protected Access (WPA) settings. The other parameter settings are standard.



Note. For information about the auto-tune parameters, see Table 19 on page 295.

Table 10: Defaults for Radio Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
11g-only	**disable**	Allows associations with 802.11g and 802.11b clients. **Note:** This parameter applies only to 802.11b/g radios.
active-scan	**enable**	Sends *probe any* requests (probe requests with a null SSID name) to solicit probe responses from other access ports. (See "Rogue Detection and Countermeasures" on page 537.)
beacon-interval	**100**	Waits 100 ms between beacons.
countermeasures	Not configured	Does not issue countermeasures against any device. (See "Rogue Detection and Countermeasures" on page 537.)
dtim-interval	**1**	Sends the delivery traffic indication map (DTIM) after every beacon.
frag-threshold	**2346**	Transmits frames up to 2346 bytes long without fragmentation.
long-retry	**5**	Sends a long unicast frame up to five times without acknowledgment.
max-rx-lifetime	**2000**	Allows a received frame to stay in the buffer for up to 2000 ms (2 seconds).
max-tx-lifetime	**2000**	Allows a frame that is scheduled for transmission to stay in the buffer for up to 2000 ms (2 seconds).

Table 10: Defaults for Radio Profile Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
preamble-length	**short**	Advertises support for short 802.11b preambles, accepts either short or long 802.11b preambles, and generates unicast frames with the preamble length specified by the client. **Note:** This parameter applies only to 802.11b/g radios.
rts-threshold	**2346**	Transmits frames longer than 2346 bytes by means of the Request-to-Send/ Clear-to-Send (RTS/CTS) method.
service-profile	No service profiles defined	Default settings for all service profile parameters, including encryption parameters, are used.
short-retry	**5**	Sends a short unicast frame up to five times without acknowledgment.
wmm	**enable**	Prioritizes traffic based on the Wi-Fi Multimedia (WMM) standard. (See "Wi-Fi Multimedia" on page 305.)

(To configure a radio profile, see "Configuring a Radio Profile" on page 267.)

RF Auto-Tuning

The RF Auto-Tuning feature dynamically assigns channel and power settings to AP radios, and adjusts those settings when needed. RF Auto-Tuning can perform the following tasks:

- Assign initial channel and power settings when an AP radio is started.
- Periodically assess the RF environment and change the channel or power setting if needed.
- Change the transmit data rate or power to maintain at least the minimum data rate with all associated clients.

By default, RF Auto-Tuning is enabled for channel configuration but disabled for power configuration.

(For more information, see "Configuring RF Auto-Tuning" on page 291.)

Default Radio Profile

WSS Software contains one default radio profile, named default. To apply common parameters to radios, you can modify the default profile or create a new one. When you create a new profile, the radio parameters in the profile are set to their factory default values.

Radio-Specific Parameters

The channel number, transmit power, and external antenna parameters are unique to each radio and are not controlled by radio profiles. Table 11 lists the defaults for these parameters.

Table 11: Radio-Specific Parameters

Parameter	Default Value	Description
channel	• 802.11g—6 • 802.11b—6 • 802.11a—Lowest valid channel number for the country of operation	Number of the channel in which a radio transmits and receives traffic
tx-power	Highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.	Transmit power of a radio, in decibels referred to 1 milliwatt (dBm)
antennatype	**internal** (The default for model AP-262 is **ANT1060**)	Nortel external antenna model **Note:** This parameter applies only to AP models that support external antennas.

Although these parameters have default values, Nortel recommends that you change the values for each radio for optimal performance. For example, leaving the channel number on each radio set to its default value can result in high interference among the radios.

(To configure these parameters, see "Configuring Radio-Specific Parameters" on page 273.)

Configuring AP access points

To configure AP access points, perform the following tasks, in this order:

- Specify the country of operation. (See “Specifying the Country of Operation” on page 248.)
- Configure a template for automatic configuration of Distributed APs. (See “Configuring a Template for Automatic AP Configuration” on page 251.)
- Configure AP access points and dual homing. (See “Configuring AP Port Parameters” on page 256.)
- Configure AP-WSS security. (See “Configuring AP-WSS Security” on page 261.)
- Configure a service profile to set SSID and encryption parameters. (See “Configuring a Service Profile” on page 265.)
- Configure a radio profile. (See “Configuring a Radio Profile” on page 267.)
- If required, configure the channel, transmit power, and external antenna type on each radio. (See “Configuring Radio-Specific Parameters” on page 273.)
- Map the radio profile to a service profile. (See “Mapping the Radio Profile to Service Profiles” on page 276.)
- Assign the radio profile to radios and enable the radios. (See “Assigning a Radio Profile and Enabling Radios” on page 277.)

Specifying the Country of Operation

You must specify the country in which you plan to operate the WSS switch and its AP access ports. WSS Software does not allow you to configure or enable the AP access point radios until you specify the country of operation.



Note. In countries where Dynamic Frequency Selection (DFS) is required, WSS Software performs the appropriate check for radar. If radar is detected on a channel, the AP radio stops using the channel for the amount of time specified in the specified country's regulations. WSS Software also generates a log message to notify you when this occurs.

To specify the country, use the following command:

set system countrycode *code*

For the country, you can specify one of the codes listed in Table 12.

Table 12: Country Codes

Country	Code
Australia	**AU**
Austria	**AT**
Belgium	**BE**
Brazil	**BR**
Canada	**CA**
China	**CN**
Czech Republic	**CZ**
Denmark	**DK**
Finland	**FI**
France	**FR**
Germany	**DE**
Greece	**GR**
Hong Kong	**HK**
Hungary	**HU**
Iceland	**IS**
India	**IN**
Ireland	**IE**
Israel	**IL**
Italy	**IT**
Japan	**JP**

Table 12: Country Codes (continued)

Country	Code
Liechtenstein	**LI**
Luxembourg	**LU**
Malaysia	**MY**
Mexico	**WSS**
Netherlands	**NL**
New Zealand	**NZ**
Norway	**NO**
Poland	**PL**
Portugal	**PT**
Saudi Arabia	**SA**
Singapore	**SG**
Slovakia	**SK**
Slovenia	**SI**
South Africa	**ZA**
South Korea	**KR**
Spain	**ES**
Sweden	**SE**
Switzerland	**CH**
Taiwan	**TW**
Thailand	**TH**
United Arab Emirates	**AE**
United Kingdom	**GB**
United States	**US**

Note. The current software version might not support all of the countries listed here. (For a list of the countries that are supported, see *Nortel Regulatory Information*.)

To verify the configuration change, use the following command:

show system

The following commands set the country code to US (United States) and verify the setting:

```
23x0# set system countrycode US
success: change accepted.

23x0# show system
================================================================================
 Product Name:       WSS-23xx
 System Name:        WSS-23xx
 System Countrycode: US
 System Location:
 System Contact:
 System IP:          30.30.30.2
 System MAC:         00:0B:0E:02:76:F6
 License:            unlimited
================================================================================
 Boot Time:          2003-05-07 08:28:39
 Uptime:                 0 days 04:00:07
================================================================================
 Fan status:  fan1 OK fan2 OK fan3 OK
 Temperature: temp1 ok  temp2 ok  temp3 ok
 PSU Status:  Lower Power Supply DC ok AC ok  Upper Power Supply missing
 Memory:      115.09/496.04 (23%)
 Total Power Over Ethernet : 32.000
================================================================================
```

Configuring a Template for Automatic AP Configuration

You can use a configuration template to deploy unconfigured Distributed APs. A Distributed AP that does not have a configuration on an WSS switch can receive its configuration from the template instead.

The template assigns a Distributed AP number and name to the AP, from among the unused valid AP numbers available on the switch. The template also configures the AP with the AP and radio parameter settings in the template. The AP and radio parameter settings in the template are configurable. (See "Configuring a Template" on page 252.)

The template does not control SSIDs, encryption parameters, or any other parameters managed by service profiles. You still need to configure a service profile separately for each SSID.

An WSS switch can have one template.

How an Unconfigured AP Finds an WSS Switch To Configure It

The boot process for a Distributed AP that does not have a configuration on an WSS switch is similar to the process for configured Distributed APs. After the AP starts up, it uses DHCP to configure its IP connection with the network. The AP then uses the IP connection to contact an WSS switch.

The WSS switch contacted by the AP determines the best switch to use for configuring the AP, and sends the AP the IP address of that switch. The best switch to use for configuring the AP is the switch that has a template with a high bias setting. If more than one WSS has a template with a high bias setting, the switch that has the greatest capacity to add new unconfigured APs is selected.

An WSS switch's capacity to add new unconfigured Distributed AP's is the lesser of the following:

- Maximum number of APs that can be configured on the switch, minus the number that are configured
- Maximum number of APs that can be active on the switch, minus the number that are active

For example, suppose the Mobility Domain has two WSS switches, with the capacities and loads listed in Table 13.

Table 13: Example WSS-2360 AP Capacities and Loads

	WSS-2360 A	WSS-2360 B
Maximum Configured	30	30
Maximum Active	12	12
Number Currently Configured	25	20
Number Currently Active	8	12

For WSS-2360 A:

- The Number of APs that can be configured on the switch, minus the number that are configured, is 30 - 25 = 5.
- The Number of APs that can be active on the switch, minus the number that are active, is 12 - 8 = 4.
- The lesser of the two values is 4. The switch can have up to 4 more APs.

For WSS-2360 B:

- The Number of APs that can be configured on the switch, minus the number that are configured, is 30 - 20 = 10.
- The Number of APs that can be active on the switch, minus the number that are active, is 12 - 12 = 0.
- The lesser of the two values is 0. The switch can have no more APs.

WSS-2360 A has the capacity to add 4 more APs, whereas WSS-2360 B cannot add any more APs. Therefore, the WSS contacted by the AP sends WSS-2360 A's IP address to the AP. The AP then requests a software image file and configuration from WSS-2360 A. WSS-2360 A sends the software image and sends configuration parameters based on the template.

Configured APs Have Precedence Over Unconfigured APs

When an WSS switch determines the WSS IP address to send to a booting AP, the switch gives preference to APs that are already configured, over unconfigured APs that require a template. The WSS can direct a configured AP to a switch that has active APs configured using the template, even if the switch does not have capacity for more active APs. In this case, the WSS randomly selects an AP using the template to disconnect, and accepts a connection from the configured AP in its place.

The disconnected AP can then begin the boot process again to find another WSS switch that has a template. When the AP is disconnected, the AP's clients experience a service disruption, and will attempt to associate with another AP if available to reconnect to the SSID they were using. If another AP is not available to a client, the client can still reconnect after the disconnected AP is connected to a new WSS and finishes the boot and configuration process.

Configuring a Template

The template for Distributed AP configuration is like an individual AP configuration, except the configuration has the name *auto* instead of a Distributed AP number.

To create a template for automatic Distributed AP configuration, type the following command:

```
23x0# set dap auto
success: change accepted.
```

To display the AP settings in the template, type the following command:

```
23x0# show dap config auto
Dap auto: mode: disabled bias: high
                                          fingerprint
           boot-download-enable: YES
           load balancing group: none
   Radio 1: type: 802.11g, mode:  enabled, channel: dynamic
   tx pwr: 15, profile: default
auto-tune max-power:default,min-client-rate:5.5,max-retransmissions:10
   Radio 2: type: 802.11a, mode:  enabled, channel: dynamic
   tx pwr: 11, profile: default
auto-tune max-power:default,min-client-rate:24,max-retransmissions:10
```

This example shows the defaults for the AP parameters you can configure in the template. Table 14 on page 253 lists the configurable template parameters and their defaults. The only parameter that requires configuration is the template mode. The template is disabled by default. To use the template to configure Distributed APs, you must enable the template. (See "Enabling the Template" on page 254.)

Table 14: Configurable Template Parameters for Distributed APs

Parameter	Default Value
AP Parameters	
mode	**disabled**
bias	**high**
upgrade-firmware (boot-download-enable)	**enable** (YES)
group (load balancing group)	none
blink (Not shown in **show dap config** output)	**disable**
Radio Parameters	
radiotype (type) (Applies only to single-radio AP models)	**11g** (or **11b** for country codes where 802.11g is not allowed)
mode	**enabled**
tx-pwr	Highest setting allowed for the country of operation
radio-profile (profile)	**default**
max-power	**default**
min-client-rate	**5.5** for 802.11b/g **24** for 802.11a
max-retransmissions	**10**

APs that receive their configurations from the template also receive the radio settings from the radio profile used by the template. Likewise, the SSIDs and encryption settings come from the service profiles mapped to the radio profile. To use a radio profile other than *default*, you must specify the radio profile you want to use. (See "Specifying the Radio Profile Used by the Template" on page 254.)

Changing AP Parameter Values

The commands for configuring AP and radio parameters for the template are the same as the commands for configuring an individual Distributed AP. Instead of specifying a Distributed AP number with the command, specify **auto**. For more information about the syntax, see the "AP access point Commands" chapter of the *Nortel WLAN 2300 System Software Command Reference*.

AP Parameters:

set dap auto mode {enable | disable}

set dap auto bias {high | low}

set dap auto upgrade-firmware {enable | disable}

set dap auto group *name*

set dap auto blink {enable | disable}

Radio Parameters:

set dap auto radiotype {11a | 11b| 11g}

set dap auto radio {1 | 2} mode {enable | disable}

set dap auto radio {1 | 2} radio-profile *name* **mode {enable | disable}**

set dap auto radio {1 | 2} auto-tune max-power *power-level*

set dap auto radio {1 | 2} auto-tune max-retransmissions *retransmissions*

set dap auto radio {1 | 2} auto-tune min-client-rate *rate*

Enabling the Template

To enable the template for automatic Distributed AP configuration, type the following command:

```
23x0# set dap auto mode enable
success: change accepted.
```

Specifying the Radio Profile Used by the Template

The template uses radio profile *default* by default. To use another radio profile instead, use the following command:

set dap auto radio {1 | 2} radio-profile *name* **mode {enable | disable}**

The following command changes the template to use radio profile *autodap1* for radio 1:

```
23x0# set dap auto radio 1 radio-profile autodap1
success: change accepted.
```

Note. You must configure the radio profile before you can apply it to the template.

Displaying Status Information for APs Configured by the Template

To display status information for APs configured by the template, type the following command:

```
23x0# show dap status auto
 Dap:100(auto),IP-addr:10.8.255.6(vlan'default'),APmodel:AP-2330,
          manufacturer: Nortel, name: DAP100
     ================================================
State:      operational
```

```
CPU info:  IBM:PPC speed=266666664 Hz version=405GPr
                id= ram=33554432
                s/n=0333703027 hw_rev=A3
Uptime:    18 hours, 36 minutes, 27 seconds

Radio1type:802.11g,state:configuresucceed[Enabled](802.11bprotect)
      operational channel: 1 operational power: 14
      base mac: 00:0b:0e:00:d2:c0
      bssid1: 00:0b:0e:00:d2:c0, ssid: public
      bssid2: 00:0b:0e:00:d2:c2, ssid: employee-net
      bssid3: 00:0b:0e:00:d2:c4, ssid: mycorp-tkip
Radio 2 type: 802.11a, state: configure succeed [Enabled]
      operational channel: 64 operational power: 14
      base mac: 00:0b:0e:00:d2:c1
      bssid1: 00:0b:0e:00:d2:c1, ssid: public
      bssid2: 00:0b:0e:00:d2:c3, ssid: employee-net
      bssid3: 00:0b:0e:00:d2:c5, ssid: mycorp-tkip
```

The output displays *auto* next to the Distributed AP number to indicate that the AP was configured using a template.

Converting an AP Configured by the Template into a Permanent AP

You can convert a temporary AP configuration created by the template into a persistent AP configuration on the WSS switch. To do so, use the following command:

set dap auto persistent {*dap-num* | **all**}

This command creates a persistent Distributed AP configuration based on the settings in the template. The Distributed AP name and number assigned by the template are used for the persistent entry. For example, if the template assigned the number 100 and the name DAP100 to the AP, the persistent configuration for the AP has the same number and name. In this case, use **100** as the *dap-num* with **show dap**, **set dap**, or **clear dap** commands.

The AP continues to operate without interruption after you enter the **set dap auto persistent** command. The next time the AP is restarted, the template is not used to configure the AP. Instead, the persistent configuration is used. (Use the **save config** command to make the AP configuration persistent across switch restarts.)

Configuring AP Port Parameters

To configure an WSS switch for connection to an AP access port, you must do one of the following:

- For an AP access point directly connected to an WSS switch port, configure the WSS switch port as an AP access port. ("Setting the Port Type for a Directly Connected AP" on page 256.)
- For an AP access point indirectly connected to an WSS switch through an intermediate Layer or Layer network, configure a Distributed AP on the WSS switch. ("Configuring an Indirectly Connected AP" on page 258.)

Optionally, you also can change other parameters that affect the entire AP:

- AP name. (See "Changing AP Names" on page 259.)
- Dual-home bias. (See "Changing Bias" on page 260.)
- Load-balancing group. (See "Configuring a Load-Balancing Group" on page 260.)
- Automatic firmware upgrade capability. (See "Disabling or Reenabling Automatic Firmware Upgrades" on page 260.)
- LED blink mode. (See "Enabling LED Blink Mode" on page 260.)

(For information about configuring RF Auto-Tuning settings on a radio, see "Configuring RF Auto-Tuning" on page 291.)

Table 15 lists how many APs you can configure on an WSS switch, and how many APs a switch can boot. The numbers are for directly connected and Distributed APs combined.

Table 15: Maximum APs Supported Per Switch

WSS Switch Model	Maximum That Can Be Configured	Maximum That Can Be Booted
WSS-2380	300	40, 80, or 120, depending on the license level
WSS-2370	100	40
WSS-2360	30	12
WSS-2350	8	3

Setting the Port Type for a Directly Connected AP

You must set the port type on WSS switch ports that are directly connected to AP access ports.

When you change port type, WSS Software applies default settings appropriate for the port type. Table 16 lists the default settings that WSS Software applies when you set a port's type to **ap**.

Table 16: AP Access Port Defaults

Port parameter	Setting
VLAN membership	Port is removed from all VLANs. You cannot assign an AP access point to a VLAN. WSS Software automatically assigns AP access points to VLANs based on user traffic.
Spanning Tree Protocol (STP)	Not applicable
802.1X	Port uses authentication parameters configured for users.
Port groups	Not applicable
IGMP snooping	Enabled as users are authenticated and join VLANs.
Maximum user sessions	Not applicable



Warning! When you set the port type for AP use, you must specify the PoE state (enable or disable) of the port. Use the WSS switch's PoE to power Nortel AP access ports only. If you enable PoE on a port connected to another device, physical damage to the device can result.



Note. You cannot configure port 7 or 8 on an WSS-2360 switch, or port 1 on an WSS-2350 , or any gigabit Ethernet port, as an AP port. To manage an AP access point on an WSS-2380 switch, configure a Distributed AP connection on the switch. (See "Configuring an Indirectly Connected AP" on page 258.)

To set the port type for AP access points, use the following command:

set port type ap *port-list*
model {AP2750 | AP-52 | AP-101 | AP-122 | AP-241 | AP-252 | AP-262 | AP-341 | AP-352 | 2330}
poe {enable | disable}
[radiotype {11a | 11b| 11g}]

You must specify the AP model and the PoE state.



Note. All AP models except the 2330 and AP2750 have been discontinued but are still supported by the command.

For models AP-101, AP-241, and AP-341, you can specify one of the following for the radio type:

- **11a**—802.11a
- **11b**—802.11b
- **11g**—802.11g (AP-241 and AP-341 only)

AP access point models AP2750, AP-241 and AP-341 have a single radio that can be configured for 802.11a or 802.11b/g. Other AP models have two radios. One radio is always 802.11a. The other radio is 802.11b/g, but can be configured for 802.11b or 802.11g exclusively. If the country of operation specified by the **set system countrycode** command does not allow 802.11g, the default is 802.11b.



Note. All AP models except the 2330 and AP2750 have been discontinued but are still supported by the command.

AP model AP-262 requires an external antenna for the 802.11b/g radio. You must specify the Nortel antenna model. AP-3*xx* models have an internal 802.1b/g antenna as well as a connector for an external antenna, so use of an external antenna is optional on these models. The 2330 also has a connector for an optional external 802.11a antenna. To specify the antenna model, use the **set {ap | dap} radio antennatype** command. (See "Configuring the External Antenna Model" on page 274.)

AP radios configured for 802.11g also allow associations from 802.11b clients by default. (To disable support for 802.11b associations, see "Disabling 802.11b Client Associations on 802.11b/g Radios" on page 270.)

To set ports 11 through 14 and port 16 for AP access point model 2330 and enable PoE on the ports, type the following command:

```
23x0# set port type ap 11-14,16 model 2330 poe enable
This may affect the power applied on the configured ports. Would you like to
continue? (y/n) [n]y
```

To set ports 5 through 8 for AP access point model AP-241, enable PoE on the ports, and set the radio type to 802.11a, type the following command:

```
23x0# set port type ap 5-8 model AP-241 poe enable radiotype 11a
This may affect the power applied on the configured ports. Would you like to
continue? (y/n) [n]y
```

Configuring an Indirectly Connected AP

If an AP access point that you want to manage using the WSS switch is indirectly connected to the switch through a Layer 2 or Layer 3 network, configure the AP using the following command:

set dap *dap-num* **serial-id** *serial-ID*
model {AP2750 | AP-52 | AP-101 | AP-122 | AP-241 | AP-252 | AP-262 | AP-341 | AP-352 | 2330}
[radiotype {11a | 11b| 11g}]

The *dap-num* parameter identifies the Distributed AP connection for the AP. The range of valid connection ID numbers depends on the WSS switch model:

- For an WSS-2380, you can specify a number from 1 to 300.
- For an WSS-2370, you can specify a number from 1 to 100.
- For an WSS-2360, you can specify a number from 1 to 30.
- For an WSSR-2350, you can specify a number from 1 to 8.

For the **serial-id** parameter, specify the serial ID of the AP. The serial ID is listed on the AP case. To display the serial ID using the CLI, use the **show version details** command.

The **model** and **radiotype** parameters have the same options as they do with the **set port type ap** command. Because the WSS switch does not supply power to an indirectly connected AP, the **set dap** command does not use the **poe** parameter.

To configure Distributed AP connection 1 for AP model 2330 with serial-ID 0322199999, type the following command:

```
23x0# set dap 1 serial-id 0322199999 model 2330
success: change accepted.
```

(To specify the external antenna type, use the **set {ap | dap} radio antennatype** command. See "Configuring the External Antenna Model" on page 274.)

To configure Distributed AP connection 2 for AP model AP-241 with serial-ID 0322188888 and radio type 802.11a, type the following command:

```
23x0# set dap 2 serial-id 0322188888 model AP-241 radiotype 11a
success: change accepted.
```

Clearing an AP from the Configuration



Warning! When you clear an AP access port, WSS Software ends user sessions that are using the AP.

To clear the port settings from a port, use the following command:

clear port type *port-list*

This command resets the port as a network port and removes all AP-related parameters from the port.



Note. The **clear port type** command does not place the cleared port in any VLAN, not even in the default VLAN (VLAN 1). To use the cleared port in a VLAN, you must add the port to the VLAN. (For instructions, see "Adding Ports to a VLAN" on page 92.)

To clear a Distributed AP, use the following command:

clear dap *dap-num*

Changing AP Names

The default name of a directly attached AP is based on the port number of the AP access point attached to the AP. For example, the default name for an AP on AP access point 1 is *AP01*. The default name of a Distributed AP is based on the number you assign to it when you configure the connection. For example, the default name for Distributed AP 1 is *DAP01*.

AP names appear in the output of some CLI **show** commands and in WLAN Management Software . To change the name of an AP, use the following command:

set {**ap** *port-list* | **dap** *dap-num*} **name** *name*

Changing Bias

The CLI commands described in this section enable you to change the bias for an AP.

To change the bias of an AP, use the following command:

set {**ap** *port-list* | **dap** *dap-num*} **bias** {**high** | **low**}

The default bias is high.

To change the bias for a Distributed AP to low, type the following command:

```
23x0# set dap 1 bias low
success: change accepted.
```

Configuring a Load-Balancing Group

A load-balancing group is a named set of AP access ports. WSS Software balances user sessions among the access ports in the group.

To assign an AP access point to a load-balancing group, use the following command:

set {**ap** *port-list* | **dap** *dap-num*} **group** *name*

To configure a load-balancing group named *loadbalance1* that contains directly-connected AP access ports on ports 1, 4, and 7, type the following command:

```
23x0# set ap 1,4,7 group loadbalance1
success: change accepted.
```

Disabling or Reenabling Automatic Firmware Upgrades

An AP access point can automatically upgrade its boot firmware by loading the upgrade version of the firmware from an WSS switch when the AP is booting. Automatic firmware upgrades are enabled by default.

To disable or reenable automatic firmware upgrades, use the following command:

set {**ap** *port-list* | **dap** *dap-num*} **upgrade-firmware** {**enable** | **disable**}

Enabling LED Blink Mode

Blink mode makes an AP easy to identify. When blink mode is enabled on AP-*xxx* models, the health and radio LEDs alternately blink green and amber. When blink mode is enabled on an AP2750, the 11a LED blinks on and off. By default, blink mode is disabled. Blink mode continues until you disable it. LED blink mode is disabled by default.

Changing the LED blink mode does not alter operation of the AP access port. Only the behavior of the LEDs is affected.

To enable or disable LED blink mode, use the following command:

set {**ap** *port-list* | **dap** *dap-num*} **blink** {**enable** | **disable**}

Configuring AP-WSS Security

WSS Software provides security for management traffic between WSS switches and Distributed APs. For Distributed APs that support this feature, all management traffic between the AP and the WSS is encrypted.

The encryption uses RSA as the public key cryptosystem, with AES-CCM for data encryption and integrity checking and HMAC-MD5 for keyed hashing and message authentication during the key exchange. Bulk data protection is provided by AES in CCM mode (AES CTR for encryption and AES-CBC-MAC for data integrity). A 64-bit Message Authentication Code is used for data integrity.

Note. This feature applies to Distributed APs only, not to directly connected APs configured on AP access ports. In addition, AP models AP-101 and AP-122 do not have encryption keys and do not support this feature regardless of how they are connected to the WSS switch.

Note. The maximum transmission unit (MTU) for encrypted AP management traffic is 1498 bytes, whereas the MTU for unencrypted management traffic is 1474 bytes. Make sure the devices in the intermediate network between the WSS switch and Distributed AP can support the higher MTU.

Encryption Key Fingerprint

APs are configured with an encryption key pair at the factory. The fingerprint for the public key is displayed on a label on the back of the AP, in the following format:

```
RSA
aaaa:aaaa:aaaa:aaaa:
aaaa:aaaa:aaaa:aaaa
```

If the AP is already installed, you can display the fingerprint in WSS Software. (See “Finding the Fingerprint” on page 262.)

Encryption Options

By default, an WSS switch can configure and manage a Distributed AP regardless of whether the AP has an encryption key, and regardless of whether you have confirmed the fingerprint by setting it in WSS Software. You can configure an WSS to require Distributed APs to have an encryption key. In this case, the switch also requires their fingerprints to be confirmed in WSS Software. When AP security is required, an AP can establish a management session with the WSS only if its fingerprint has been confirmed by you in WSS Software.

Table 17 lists the AP security options and whether an AP can establish a management session with an WSS based on the option settings.

Table 17: AP Security Requirements

AP Security Setting	AP Has Fingerprint?	Fingerprint Confirmed in WSS Software?	AP Can Establish Management Session with Switch?
AP Security Required	Yes	Yes	Yes
		No	No
	No	Not Applicable	No
AP Security Optional	Yes	Yes	Yes1
		No	Yes[1]
	No	Not Applicable	Yes

1. WSS Software generates a log message listing the AP serial number and fingerprint so you can verify the AP's identity. (See "Fingerprint Log Message" on page 264.)

Confirming an AP's Fingerprint on an WSS Switch

To confirm an AP's fingerprint, find the fingerprint and use the **set dap fingerprint** command to enter the fingerprint in WSS Software.

Finding the Fingerprint

An AP's fingerprint is listed on a label on the back of the AP. (See "Encryption Key Fingerprint" on page 261.)

If the AP is already installed and operating, use the **show dap status** command to display the fingerprint. The following example shows information for Distributed AP 8, including its fingerprint:

```
23x0# show dap status 8
Dap: 8, IP-addr: 10.2.26.40 (vlan 'default'), AP model: 2330,
         manufacturer: Nortel, name: DAP08
 fingerprint:b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
======================================================
State:     operational (insecure)
CPU info:  IBM:PPC speed=266666664 Hz version=405GPr
                  id=0x29f1886d447f111a ram=33554432
                  s/n=0424000779 hw_rev=A3
Uptime:    1 hours, 8 minutes, 17 seconds

Radio 1 type: 802.11g, state: configure succeed [Enabled]
       operational channel: 1 operational power: 1
       base mac: 00:0b:0e:0a:60:00
       bssid1: 00:0b:0e:0a:60:00, ssid: public
       bssid2: 00:0b:0e:0a:60:02, ssid: nortel
```

```
Radio 2 type: 802.11a, state: configure succeed [Enabled]
       operational channel: 48 operational power: 11
       base mac: 00:0b:0e:0a:60:01
       bssid1: 00:0b:0e:0a:60:01, ssid: public
       bssid2: 00:0b:0e:0a:60:03, ssid: nortel
```

The fingerprint is displayed regardless of whether it has been confirmed in WSS Software.



Note. The **show dap config** command lists an AP's fingerprint only if the fingerprint has been confirmed in WSS Software. If the fingerprint has not been confirmed, the fingerprint info in the command output is blank.

Confirming a Fingerprint on the Switch

To confirm an AP's fingerprint on an WSS switch, use the following command:

set dap *num* **fingerprint** *hex*

where *hex* is the 16-digit hexadecimal number of the fingerprint. Use a colon between each digit. Make sure the fingerprint you enter matches the fingerprint used by the AP.

The following example sets the fingerprint for Distributed AP 8:

```
23x0# set dap 8 fingerprint b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
success: change accepted.
```

Setting the AP Security Requirement on an WSS Switch

You can configure the WSS to require all Distributed APs to have encryption keys. In this case, the WSS does not establish a management session with a Distributed AP unless the AP has a key, and you have confirmed the key's fingerprint in WSS Software.



Note. A change to AP security support does not affect management sessions that are already established. To apply the new setting to an AP, restart the AP.

To configure AP security requirements, use the following command:

set dap security {require | optional}

The following command configures an WSS to require Distributed APs to have encryption keys:

```
23x0# set dap security require
```

Fingerprint Log Message

If AP encryption is optional, and an AP whose fingerprint has not been confirmed in WSS Software establishes a management session with the WSS, WSS Software generates a log message such as the following:

```
DAP-HS:(secure optional)configure DAP 0335301065 with fingerprint
    c6:98:9c:41:32:ab:37:09:7e:93:79:a4:ca:dc:ec:fb
```

The message lists the serial number and fingerprint of the AP. You can check this information against your records to verify that the AP is authentic.

Configuring a Service Profile

A service profile is a set of parameters that control advertisement (beaconing) and encryption for an SSID.

This section describes how to create a service profile and set SSID parameters. To configure encryption parameters, see "Configuring User Encryption" on page 191.

(To display service profile information, see "Displaying Service Profile Information" on page 286.)

To create a service profile and assign an SSID to it, use the following command:

set service-profile *name* **ssid-name** *ssid-name*

An SSID can be up to 32 alphanumeric characters long and cannot contain blanks.

The following command configures a service profile named *corp1*, and assigns SSID *mycorp_rnd* to it:

```
23x0# set service-profile corp1 ssid-name mycorp_rnd
success: change accepted.
```

Disabling or Reenabling Encryption for an SSID

To specify whether the SSID is encrypted or unencrypted, use the following command:

set service-profile *name* **ssid-type** [**clear** | **crypto**]

The default is crypto.

Disabling or Reenabling Beaconing of an SSID

To specify whether the SSID is beaconed, use the following command:

set service-profile *name* **beaconed** {**enable** | **disable**}

SSIDs are beaconed by default.

An AP radio responds to an 802.11 *probe any* request only for a beaconed SSID. A client that sends a *probe any* request receives a separate response for each of the beaconed SSIDs supported by a radio. For a nonbeaconed SSID, radios respond only to directed 802.11 probe requests that match the nonbeaconed SSID's SSID string.

When you disable beaconing for an SSID, the radio still sends beacon frames, but the SSID name in the frames is blank.

Changing the Fallthru Authentication Type

By default, WSS Software uses Web-based AAA for users who do not match an 802.1X or MAC authentication rule, and therefore *fall through* these authentication types. You can change the *fallthru* method to last-resort or none.

To change the fallthru method, use the following command:

set service-profile *name* **auth-fallthru** {**last-resort** | **none** | **web-portal**}

(For more information about network user authentication, see “Configuring AAA for Network Users” on page 401.)

Configuring a Radio Profile

A radio profile is a set of parameters that apply to multiple radios. You can easily assign configuration parameters to many radios by configuring a profile and assigning the profile to the radios.

To configure a radio profile:

- Create a new profile.
- Change radio parameters.
- Map the radio profile to one or more service profiles.

(For a list of the parameters controlled by radio profiles and their defaults, see Table 10 on page 244.)

The channel number, transmit power, and external antenna type are unique to each radio and are not controlled by radio profiles. (To configure these parameters, see "Configuring Radio-Specific Parameters" on page 273.)

(To display radio profile information, see "Displaying Radio Profile Information" on page 287.)

Creating a New Profile

To create a radio profile, use the following command:

set radio-profile *name* **[mode {enable | disable}]**

Specify a name of up to 16 alphanumeric characters. Do not include the **mode enable** or **mode disable** option.

After you create the radio profile, you can use the **enable** and **disable** options to enable or disable all radios that use the profile.

To configure a new radio profile named *rp1*, type the following command:

```
23x0# set radio-profile rp1
success: change accepted.
```

To assign the profile to one or more radios, use the **set ap radio radio-profile** command. (See "Assigning a Radio Profile and Enabling Radios" on page 277.)

Changing Radio Parameters

To change individual parameters controlled by a radio profile, use the commands described in the following sections.

Note. You must disable all radios that are using a radio profile before you can change parameters in the profile. (See "Disabling or Reenabling All Radios Using a Profile" on page 279.)

Changing the Beacon Interval

The beacon interval is the rate at which a radio advertises its beaconed SSID(s). To change the beacon interval, use the following command:

set radio-profile *name* **beacon-interval** *interval*

The interval can be a value from 25 ms through 8191 ms. The default is 100.

The beacon interval does not change even when advertisement is enabled for multiple SSIDs. WSS Software still sends one beacon for each SSID during each beacon interval.

To change the beacon interval for radio profile *rp1* to 200 ms, type the following command:

```
23x0# set radio-profile rp1 beacon-interval 200
success: change accepted.
```

Changing the DTIM Interval

The DTIM interval specifies the number of times after every beacon that a radio sends a delivery traffic indication map (DTIM). An AP access point sends the multicast and broadcast frames stored in its buffers to clients who request them in response to the DTIM. The DTIM interval applies to both the beaconed SSID and the unbeaconed SSID.

The DTIM interval does not apply to unicast frames. An AP access point also stores unicast frames in buffer memory, but the AP includes information about the buffered unicast frames in each beacon frame. When a user station receives a beacon frame that advertises unicast frames destined for the station, the station sends a request for the frames and the AP transmits the requested frames to the user station.

To change the DTIM interval, use the following command:

set radio-profile *name* **dtim-interval** *interval*

The interval can be a value from 1 through 31. The default is 1.

To change the DTIM interval for radio profile *rp1* to 2, type the following command:

```
23x0# set radio-profile rp1 dtim-interval 2
success: change accepted.
```

Changing the RTS Threshold

The RTS threshold specifies the maximum length a frame can be before a radio uses the Request-to-Send/Clear-to-Send (RTS/CTS) method to send the frame. The RTS/CTS method clears the air of other traffic to avoid corruption of the frame due to a collision with another frame.

When a frame is long enough for the RTS/CTS method to be applicable, the radio sends a Request-To-Send (RTS) message addressed to the intended receiver for the frame. The receiver replies with a Clear-To-Send (CTS) message. When the radio receives the CTS message, the radio transmits the frame and waits for an acknowledgment from the receiver. The radio does not transmit additional frames until receiving the acknowledgment.

Any other user station that overhears the RTS or CTS message stops transmitting until the station overhears the acknowledgment message.

To change the RTS threshold, use the following command:

set radio-profile *name* **rts-threshold** *threshold*

The threshold can be a value from 256 bytes through 3000 bytes. The default is 2346.

To change the RTS threshold for radio profile *rp1* to 1500 bytes, type the following command:

```
23x0# set radio-profile rp1 rts-threshold 1500
success: change accepted.
```

Changing the Fragmentation Threshold

The fragmentation threshold specifies the longest a frame can be without being fragmented into multiple frames by a radio before transmission. To change the fragmentation threshold, use the following command:

set radio-profile *name* **frag-threshold** *threshold*

The threshold can be a value from 256 through 2346. The default is 2346.

To change the fragmentation threshold for radio profile *rp1* to 1500 bytes, type the following command:

```
23x0# set radio-profile rp1 frag-threshold 1500
success: change accepted.
```

Changing the Short Retry Threshold

The short retry threshold specifies the number of times a radio can send a short unicast frame without receiving an acknowledgment for the frame. A short unicast frame is a frame that is *shorter* than the RTS threshold.

To change the short retry threshold, use the following command:

set radio-profile *name* **short-retry** *threshold*

The threshold can be a value from 1 through 15. The default is 5.

To change the short retry threshold for radio profile *rp1* to 3, type the following command:

```
23x0# set radio-profile rp1 short-retry 3
success: change accepted.
```

Changing the Long Retry Threshold

The long retry threshold specifies the number of times a radio can send a long unicast frame without receiving an acknowledgment for the frame. A long unicast frame is a frame that is *equal to or longer than* the RTS threshold.

To change the long retry threshold, use the following command:

set radio-profile *name* **long-retry** *threshold*

The threshold can be a value from 1 through 15. The default is 5.

To change the long retry threshold for radio profile *rp1* to 8, type the following command:

```
23x0# set radio-profile rp1 long-retry 8
success: change accepted.
```

Changing the Maximum Receive Threshold

The maximum receive threshold specifies the number of milliseconds a frame *received* by a radio can remain in buffer memory. To change the maximum receive lifetime, use the following command:

set radio-profile *name* **max-rx-lifetime** *time*

The time can be from 500 ms (0.5 second) through 250,000 ms (250 seconds). The default is 2000 ms (2 seconds).

To change the maximum receive threshold for radio profile *rp1* to 4000 ms, type the following command:

```
23x0# set radio-profile rp1 max-rx-lifetime 4000
success: change accepted.
```

Changing the Maximum Transmit Threshold

The maximum transmission threshold specifies the number of milliseconds a frame *scheduled to be transmitted* by a radio can remain in buffer memory. To change the maximum transmit lifetime, use the following command:

set radio-profile *name* **max-tx-lifetime** *time*

The time can be from 500 ms (0.5 second) through 250,000 ms (250 seconds). The default is 2000 ms (2 seconds).

To change the maximum transmit threshold for radio profile *rp1* to 4000 ms, type the following command:

```
23x0# set radio-profile rp1 max-tx-lifetime 4000
success: change accepted.
```

Disabling 802.11b Client Associations on 802.11b/g Radios

By default, an 802.11b/g radio allows associations from 802.11b clients as well as 802.11g clients. The radio requires a client to support the 802.11b data rates but client support for the higher 802.11g rates is optional. This radio configuration allows both types of clients to associate with the radio and is useful in networks that have a mixture of both types of clients.

When 802.11b traffic is detected by an 802.11b/g radio, the radio enters protection mode. Protection mode guards against 802.11b interference with 802.11g traffic that is at data rates higher than the 802.11b rates. Because 802.11b clients cannot detect the traffic at data rates higher than are supported by 802.11b, the clients might cause interference by sending traffic while 802.11g access ports or clients also are sending traffic.

To guard against interference, an 802.11b/g radio in protection mode sends messages while 802.11g traffic at higher data rates is being sent, to inform 802.11b devices about the 802.11g traffic and reserve bandwidth for the traffic. Protection mode remains in effect until 60 seconds after the last 802.11b traffic is detected by the 802.11b/g radio.

Protection mode lowers overall traffic throughput due to the additional messages sent by 802.11b/g radios. You can configure the 802.11b/g radios in a radio profile to reject association attempts by 802.11b clients so

that protection mode is less likely to be required. In this case, the 802.11b/g radios require a client to support all the 802.11g rates.



Note. Even when association of 802.11b clients is disabled, if an 802.11b/g radio detects a beacon from an 802.11b network, the radio enters protection mode to protect against interference.

To configure 802.11b/g radios to reject association attempts from 802.11b clients, use the following command:

set radio-profile *name* **11g-only {enable | disable}**

To configure the 802.11b/g radios in radio profile *rp1* to allow associations from 802.11g clients only, type the following command:

```
23x0# set radio-profile rp1 11g-only enable
success: change accepted.
```

Changing the Preamble Length

By default, 802.11b/g radios advertise support for frames with short preambles and can support frames with short or long preambles.

An 802.11b/g radio generates unicast frames to send to a client with the preamble length specified by the client. An 802.11b/g radio always uses a long preamble in beacons, probe responses, and other broadcast or multicast traffic.

Generally, clients assume access ports require long preambles and request to use short preambles only if the access point with which they are associated advertises support for short preambles. You can disable the advertisement of support for short preambles by setting the preamble length value to **long**. In this case, clients assume that the access point supports long preambles only and the clients request long preambles.

Changing the preamble length value affects only the support advertised by the radio. Regardless of the preamble length setting (**short** or **long**), an 802.11b/g radio accepts and can generate 802.11b/g frames with either short or long preambles.

If any client associated with an 802.11b/g radio uses long preambles for unicast traffic, the AP access point still accepts frames with short preambles but does not transmit any frames with short preambles. This change also occurs if the access point overhears a beacon from an 802.11b/g radio on another access point that indicates the radio has clients that require long preambles.

The default preamble length value is **short**. This command does not apply to 802.11a radios.

To change the preamble length advertised by 802.11b/g radios, use the following command:

set radio-profile *name* **preamble-length {long | short}**

To configure 802.11b/g radios that use the radio profile *rp_long to* advertise support for long preambles instead of short preambles, type the following command:

```
23x0# set radio-profile rp_long preamble-length long
success: change accepted.
```

Resetting a Radio Profile Parameter to its Default Value

To reset a radio profile parameter to its default value, use the following command:

clear radio-profile *name parameter*

The *parameter* can be one of the radio profile parameters listed in Table 10 on page 244.

Caution! Make sure you specify the radio profile parameter you want to reset. If you do not specify a parameter, WSS Software deletes the entire profile from the configuration.

All radios that use this profile must be disabled before you can delete the profile. If you specify a parameter, the setting for the parameter is reset to its default value. The settings of the other parameters are unchanged and the radio profile remains in the configuration. If you do not specify a parameter, the entire radio profile is deleted from the configuration.

To disable the radios that are using radio profile *rp1* and reset the **beaconed-ssid** parameter to its default value, type the following commands:

```
23x0# set radio-profile rp1 mode disable

23x0# clear radio-profile rp1 beaconed-ssid
success: change accepted.
```

Removing a Radio Profile

To remove a radio profile, use the following command:

clear radio-profile *name*

Note. You must disable all radios that are using a radio profile before you can remove the profile. (See "Disabling or Reenabling All Radios Using a Profile" on page 279.)

To disable the radios that are using radio profile *rptest* and remove the profile, type the following commands:

```
23x0# set radio-profile rptest mode disable

23x0# clear radio-profile rptest
success: change accepted.
```

Configuring Radio-Specific Parameters

The following parameters are specific to individual radios and are not controlled by a radio profile:

- Channel number
- Transmit power (in decibels referred to 1 milliwatt)
- External antenna model (if applicable)

These parameters have the following defaults:

- Channel number:
    - The default channel number for 802.11b/g is 6.
    - The default channel number for 802.11a is the lowest valid channel number for the country of operation.
- Transmit power—Highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower
- External antenna model—internal antenna used by default (except the AP-262, which uses ANT1060 by default)

Configuring the Channel and Transmit Power



Note. If RF Auto-Tuning is enabled for channels or power, you cannot set the channels or power manually using the commands in this section. See "Configuring RF Auto-Tuning" on page 291.

To set the channel and transmit power of a radio, use the following commands:

set {**ap** *port-list* | **dap** *dap-num*} **radio** {**1** | **2**} **channel** *channel-number*

set {**ap** *port-list* | **dap** *dap-num*} **radio** {**1** | **2**} **tx-power** *power-level*

The parameters are shown in separate commands for simplicity. However, you can use the **channel** and **tx-power** parameters on the same command line.

Specify **1** or **2** for the radio number:

- For an MP-241, MP-341, or MP-101, specify **radio 1**.
- For an 802.11b/g radio on an MP-252, MP-262, or MP-352, or an 802.11b radio on an MP-122, specify **radio 1**.
- For an 802.11a radio on an MP-252, MP-262, MAP-352, or MP-122, specify **radio 2**.



Note. The maximum transmit power you can configure on any Nortel radio is the highest setting allowed for the country of operation or the highest setting supported on the hardware, whichever is lower.

To configure the 802.11b radio on port 11 for channel 1 with a transmit power of 10 dBm, type the following command:

```
23x0# set ap 11 radio 1 channel 1 tx-power 10
success: change accepted.
```

To configure the 802.11a radio on port 5 for channel 36 with a transmit power of 10 dBm, type the following command:

```
23x0# set ap 5 radio 2 channel 36 tx-power 10
success: change accepted.
```

You also can change the channel and transmit power on an individual basis.

Configuring the External Antenna Model

The 2330 has connectors for attaching optional external 802.11a or 802.11b/g antennas. The 802.11b/g radios in AP models AP-341 and AP-352 have an internal antenna but can use an external antenna. The AP-262 802.11b/g radio requires a Nortel external antenna.

All AP-3*xx* models use the internal antennas by default. The 802.11b/g radio in an AP-262 uses external antenna model ANT-1060 by default.

Table 18 lists the external antenna models you can use with these APs.

Table 18: Nortel External Antenna Models

Model	Type	Beamwidth	
		Horizontal	Vertical
ANT-5060 (ASTN6S)1	802.11a	60°	14°
ANT-5120 (ASTN6T)	802.11a	120°	14°
ANT-5180 (ASTN6H)	802.11a	180°	14°
ANT-1060	802.11b/g	60°	65°
ANT-1120	802.11b/g	120°	60°
ANT-1180	802.11b/g	180°	40°

1. The numbers in parentheses are the numbers that appear on the back of an 802.11a antenna's reflector plate. To verify an 802.11a external antenna's model number, look for the number in parentheses.

To specify the external antenna model, use the following command:

set {**ap** *port-list* | **dap** *dap-num*} **radio**
{**1 antennatype ANT1060** | **ANT1120** | **ANT1180** | **internal**} |
{**2 antennatype ANT5060** | **ANT5120** | **ANT5180** | **internal**}

To configure antenna model ANT-1060 for a 2330 on Distributed AP 1, type the following command:

```
23x0# set dap 1 radio 1 antennatype ANT1060
success: change accepted.
```

Mapping the Radio Profile to Service Profiles

To assign SSIDs to radios, you must map the service profiles for the SSIDs to the radio profile that is assigned to the radios.

To map a radio profile to a service profile, use the following command:

set radio-profile *name* **service-profile** *name*

The following command maps service-profile *wpa_clients* to radio profile *rp2*:

```
23x0# set radio-profile rp2 service-profile wpa_clients
success: change accepted.
```

Assigning a Radio Profile and Enabling Radios

To assign a radio profile to radios, use the following command:

set {ap *port-list* **| dap** *dap-num***} radio {1 | 2} radio-profile** *name*
mode {enable | disable}

To assign radio profile *rp1* to radio 1 on ports 5-8, 11-14, and 16 and enable the radios, type the following command:

```
23x0# set ap 5-8,11-14,16 radio 1 radio-profile rp1 mode enable
success: change accepted.
```

To assign radio profile *rp1* to radio 2 on ports 11-14 and port 16 and enable the radios, type the following command:

```
23x0# set ap 11-14,16 radio 2 radio-profile rp1 mode enable
success: change accepted.
```

To disable radio 1 on port 6 without disabling the other radios using radio profile *rp1*, type the following command:

```
23x0# set ap 6 radio 1 radio-profile rp1 mode disable
```

(To disable or reenable all radios that are using a radio profile, see "Disabling or Reenabling All Radios Using a Profile" on page 279.)

Disabling or Reenabling Radios

You can disable or reenable radios on a radio profile basis or individual basis. You also can reset a radio to its factory default settings.

(To disable or reenable radios when assigning or removing a radio profile, see "Assigning a Radio Profile and Enabling Radios" on page 277.)

Enabling or Disabling Individual Radios

To disable or reenable an AP access point radio, use the following command:

set {ap *port-list* **| dap** *dap-num***} radio {1 | 2} mode {enable | disable}**

To disable radio 2 on port 3 and 7, type the following command:

```
23x0# set ap 3,7 radio 2 mode disable
success: change accepted.
```

Disabling or Reenabling All Radios Using a Profile

To disable or reenable all radios that are using a radio profile, use the following command:

set radio-profile *name* **[mode {enable | disable}]**

The following command enables all radios that use radio profile *rp1*:

```
23x0# set radio-profile rp1 mode enable
success: change accepted.
```

The following commands disable all radios that use radio profile *rp1*, change the beacon interval, then reenable the radios:

```
23x0# set radio-profile rp1 mode disable
success: change accepted.

23x0# set radio-profile rp1 beacon-interval 200
success: change accepted.

23x0# set radio-profile rp1 mode enable
success: change accepted.
```

Resetting a Radio to its Factory Default Settings

To disable an AP radio and reset it to its factory default settings, use the following command:

clear {ap *port-list* **| dap** *dap-num***} radio {1 | 2 | all}**

This command performs the following actions:

- Sets the transmit power, channel, and external antenna type to their default values.
- Removes the radio from its radio profile and places the radio in the default radio profile.

This command does not affect the PoE setting.

To disable and reset radio 2 on the AP access point connected to port 3, type the following command:

23x0# clear ap 3 radio 2

Restarting an AP

To restart an AP access port, use the following command:

reset {**ap** *port-list* | **dap** *dap-num*}

Use the **reset ap** command to reset an AP access point configured on an AP access port. Use the **reset dap** command to reset a Distributed AP.

When you enter one of these commands, the AP access point drops all sessions and reboots.



Warning! Restarting an AP can cause data loss for users who are currently associated with the AP.

Displaying AP Information

You can display the following AP information:

- AP and radio-specific configuration settings
- List of Distributed APs configured in the Mobility Domain
- List of Distributed APs that are not configured on a WSS
- Connection information for Distributed APs
- Service profile information
- Radio profile information
- Status information
- Statistics counters

Displaying AP Configuration Information

To display configuration information, use the following commands:

show ap config [*port-list* **[radio {1 | 2}]]**

show dap config [*dap-num* **[radio {1 | 2}]]**

The command lists information separately for each AP access port.

To display configuration information for an AP access point on WSS port 2, type the following command:

```
23x0# show ap config 2
Port  2: AP model: 2330, POE:  enable, bias: high, name: AP02
           boot-download-enable: YES
           load balancing group: none
  Radio 1: type: 802.11g, mode: disabled, channel:  6
  tx pwr:  1, profile: default
 auto-tune max-power: default, min-client-rate: 5.5, max-retransmissions: 10
  Radio 2: type: 802.11a, mode: disabled, channel: 36
  tx pwr:  1, profile: default
 auto-tune max-power: default, min-client-rate: 24, max-retransmissions: 10
```

To display configuration information for a Distributed AP access point configured on connection 1, type the following command:

```
23x0# show dap config 1
Dap  1: serial-id:   12345678, AP model: 2330, bias: high, name: DAP01
        fingerprint: b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
        boot-download-enable: YES
        load balancing group: none
  Radio 1: type: 802.11g, mode: disabled, channel:  6
  tx pwr:  1, profile: default
 auto-tune max-power: default, min-client-rate: 5.5, max-retransmissions: 10
  Radio 2: type: 802.11a, mode: disabled, channel: 36
  tx pwr:  1, profile: default
 auto-tune max-power: default, min-client-rate: 24, max-retransmissions: 10
```

(For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

Displaying a List of Distributed APs

To display a list of the Distributed APs configured on WSS switches in the Mobility Domain, use the following command:

show dap global [*dap-num* | **serial-id** *serial-ID*]

This command lists the System IP addresses of all the WSS switches on which each Distributed AP is configured, and lists the bias for the AP on each switch. For each Distributed AP that is configured on the switch on which you use the command, the connection number is also listed.

To display information for all Distributed APs configured on all WSS switches in the Mobility Domain, type the following command:

```
23x0# show dap global
Total number of entries: 8
DAP Serial Id   WSS IP Address   Bias
--- ----------- --------------- ----
1   11223344    10.3.8.111      HIGH
-   11223344    10.4.3.2        LOW
2   332211      10.3.8.111      LOW
-   332211      10.4.3.2        HIGH
17  0322100185  10.3.8.111      HIGH
-   0322100185  10.4.3.2        LOW
18  0321500120  10.3.8.111      LOW
-   0321500120  10.4.3.2        HIGH
```

This command indicates that the Mobility Domain contains four Distributed APs, with serial IDs *11223344*, *332211*, *0322100185*, and *0321500120*. Each AP is configured on two WSS switches, with system IP addresses 10.3.8.111 and 10.4.3.2. The bias for the AP on each WSS switch is listed. Normally, a Distributed AP boots from the WSS switch with the high bias for the AP. (For more information, see "Resiliency and Dual-Homing Options for APs" on page 227 and "AP Boot Process" on page 231.)

The DAP field indicates the connection number of each AP on the WSS switch on which the command is typed. A hyphen (-) in the DAP field indicates that the AP is configured on another WSS switch in the same Mobility Domain.

Displaying a List of Distributed APs that Are Not Configured

To display a list on Distributed APs that are not configured, use the following command:

show dap unconfigured

The following command displays information for two Distributed APs that are not configured:

```
23x0# show dap unconfigured
Total number of entries: 2
Serial Id   Model  IP Address      Port Vlan
----------- ------ --------------- ---- --------
0333001287  MP-101 10.3.8.54       5    default
0333001285  MP-122 10.3.8.57       7    vlan-eng
```

Displaying Connection Information for Distributed APs

A Distributed AP can have only one active data connection. To display the system IP address of the WSS that has the active connection, use the following command:

show dap connection [*dap-num* | **serial-id** *serial-ID*]

The **serial-id** parameter displays the active connection for a Distributed AP even if that AP is not configured on this WSS. However, if you use the command with the *dap-num* parameter or without a parameter, connection information is displayed only for Distributed APs that are configured on this WSS.

Displaying Service Profile Information

To display service profile information, use the following command:

show service-profile {*name* | **?**}

Entering **show service-profile ?** displays a list of the service profiles configured on the switch.

To display information for service profile *wpa_clients*, type the following command:

```
23x0# show service-profile wpa_clients
ssid-name:          nortel    ssid-type:           crypto
beacon:                yes    auth-fallthru:  web-portal
WEP Key 1 value:    <none>    WEP Key 2 value:    <none>
WEP Key 3 value:    <none>    WEP Key 4 value:    <none>
WEP Unicast Index:       1    WEP Multicast Index:     1
Shared Key Auth:        NO
WPA enabled:
    ciphers: cipher-tkip
    authentication: 802.1X
    TKIP countermeasures time: 60000ms
```

(For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

Displaying Radio Profile Information

To display radio profile information, use the following command:

show radio-profile {*name* | **?**}

Entering **show radio-profile ?** displays a list of radio profiles.

To display radio profile information for the default radio profile, type the following command:

```
23x0# show radio-profile default
Beacon Interval:           100   DTIM Interval:                    1
Max Tx Lifetime:          2000   Max Rx Lifetime:               2000
RTS Threshold:            2346   Frag Threshold:                2346
Short Retry Limit:           5   Long Retry Limit:                 5
Long Preamble:              NO   Allow 802.11g clients only:      NO
Tune Channel:               no   Tune Power:                      no
Tune Channel Interval:    3600   Tune Power Interval:            600
Power Backoff Timer:        10   Channel Holddown:               300
Countermeasures:          none   Active-Scan:                    yes
WMM enabled:                yes
Service profiles: default-dot1x, default-clear
```

(For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

Displaying AP Status Information

To display status information including link state and WSS status, use the following commands:

show ap status [terse] | [*port-list* | all [radio {1 | 2}]]

show dap status [terse] | [*dap-num* | all [radio {1 | 2}]]

The **terse** option displays a brief line of essential status information for each directly connected AP or Distributed AP.

The **all** option displays information for all directly attached AP access ports and all Distributed AP access ports configured on the switch.

The following command displays the status of a Distributed AP access port:

```
23x0# show dap status 1
Dap: 1, IP-addr: 10.2.30.5 (vlan 'vlan-corp'), AP model: AP-352,
         manufacturer: Nortel, name: DAP01
       fingerprint: b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
==================================================
State:     operational
CPU info:  IBM:PPC speed=266666664 Hz version=405GPr
                 id=0x29c15335347f1919 ram=33554432
                 s/n=0333703027 hw_rev=A3
Uptime:    18 hours, 36 minutes, 27 seconds

Radio1type:802.11g,state:configuresucceed[Enabled](802.11bprotect)
      operational channel: 1 operational power: 14
      base mac: 00:0b:0e:00:d2:c0
      bssid1: 00:0b:0e:00:d2:c0, ssid: public
      bssid2: 00:0b:0e:00:d2:c2, ssid: employee-net
      bssid3: 00:0b:0e:00:d2:c4, ssid: mycorp-tkip
Radio 2 type: 802.11a, state: configure succeed [Enabled]
      operational channel: 64 operational power: 14
      base mac: 00:0b:0e:00:d2:c1
      bssid1: 00:0b:0e:00:d2:c1, ssid: public
      bssid2: 00:0b:0e:00:d2:c3, ssid: employee-net
      bssid3: 00:0b:0e:00:d2:c5, ssid: mycorp-tkip
```

(For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

Displaying AP Statistics Counters

To display AP statistics counters, use the following commands:

show ap counters [*port-list* **[radio {1 | 2}]]**

show dap counters [*dap-num* **[radio {1 | 2}]]**

To display statistics counters for an AP access point on port 7, type the following command:

```
23x0# show ap counters 7
Port: 7                 radio: 1
================================
LastPktXferRate         2         PktTxCount          91594255
NumCntInPwrSave         4294966683MultiPktDrop        0
LastPktRxSigStrength    -54       MultiBytDrop        0
LastPktSigNoiseRatio    40        User Sessions       5
TKIP Pkt Transfer Ct    0         MIC Error Ct        0
TKIP Pkt Replays        0         TKIP Decrypt Err    0
CCMP Pkt Decrypt Err    0         CCMP Pkt Replays    0
CCMP Pkt Transfer Ct    0         RadioResets         0

     TxUniPkt     TxUniByte        RxPkt  RxByte   UndcrptPkt
           TxMultiPkt     TxMultiByte                   UndcrptByte
                                                          PhyError
 1.0: 164492     0  9631741       0 405041  8913512    0     0 13963
 2.0:    603     0   248716       0 191103  4608065    0     0 30547
 5.5: 370594 52742 27616521 4445625   2427   133217    0     0   723
11.0:   8016     0  2590353       0  85479  3897587    0     0  1195
TOTL: 543705 52742 40087331 4445625 684050 17552381    0     0 46441

Port: 7                 radio: 2
================================
LastPktXferRate         24        PktTxCount          374415
NumCntInPwrSave         616       MultiPktDrop        0
LastPktRxSigStrength    -80       MultiBytDrop        0
LastPktSigNoiseRatio    6         User Sessions       0
TKIP Pkt Transfer Ct    0         MIC Error Ct        0
TKIP Pkt Replays        0         TKIP Decrypt Err    0
CCMP Pkt Decrypt Err    0         CCMP Pkt Replays    0
CCMP Pkt Transfer Ct    0         RadioResets         0

     TxUniPkt    TxUniByte       RxPkt  RxByte  UndcrptPkt
           TxMultiPkt    TxMultiByte                UndcrptByte
                                                      PhyError
 6.0:   1888    0   632537      0  89354 1947920    0     0    421
 9.0:    508    0   149925      0      0       0    0     0      0
12.0:     16    0      768      0      3     681    0     0      1
18.0:    240    0    80769      0      5    1017    0     0      0
24.0: 107057 7694  8085317 629107   1663   63543    0     0 141546
```

```
36.0:    453    0   132499      0    254   20533    0    0      1
48.0:   1152    0   601435      0   1303   65461    0    0     27
54.0:   5351    0  1960146      0  19533 1269084    0    0    904
TOTL: 116665 7694 11643396 629107 112115 3368239    0    0 142900
```

(For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

To display statistics counters and other information for individual user sessions, use the **show sessions network** command. (For information, see "Managing Sessions" on page 507.)

Configuring RF Auto-Tuning

RF Auto-Tuning Overview 291
Changing RF Auto-Tuning Settings 296
Displaying RF Auto-Tuning Information 300

RF Auto-Tuning Overview

The RF Auto-Tuning feature dynamically assigns channel and power settings to AP radios, and adjusts those settings when needed. RF Auto-Tuning can perform the following tasks:

- Assign initial channel and power settings when an AP radio is started.
- Periodically assess the RF environment and change the channel or power setting if needed.
- Change the transmit data rate or power to maintain at least the minimum data rate with all associated clients.

By default, RF Auto-Tuning is enabled for channel configuration and disabled for power configuration.

Initial Channel and Power Assignment

The following process is used to assign the channel and power to an AP radio when it is first enabled:

- If RF Auto-Tuning is *disabled* for both channel and power assignment, the radio uses the channel and power settings in the radio profile that manages the radio. After this, the channel and power do not change unless you change the settings in the radio profile, or enable RF Auto-Tuning.
- If RF Auto-Tuning is *enabled* for channel and power assignment, the radio performs an RF scan and reports the results to the WSS switch that is managing the AP the radio is on. The scan results include third-party access ports. Based on the scan results, WSS Software sets the channel and power on the radio. WSS Software always selects channel and power settings that are valid for the country of operation.

    - Initial channel assignment—WSS Software determines a radio's initial channel based on RSSI values, interference levels on each valid channel, and other parameters.

      WSS Software periodically reevaluates the channel and changes it if needed.

    - Initial power assignment—The AP determines a radio's initial power level by inspecting the RSSI values of probe responses the radio receives as it actively scans channels. After all channels are scanned, the AP selects the highest RSSI value of all probe responses, and designates its sender as the radio's *nearest neighbor AP*. The AP determines the power level at which the nearest neighbor AP's probe response was sent, and uses this value and the RSSI to compute the minimum transmit power required to reach the nearest neighbor AP. This power level becomes the radio's default power level.

      The radio can temporarily increase its power level based on client needs but returns to its default power level when clients no longer need the higher power level.

      WSS Software periodically reevaluates the default power level and changes it if needed.

Channel and Power Tuning

RF Auto-Tuning can change the channel or power of a radio, to compensate for RF changes such as interference, or to maintain at least the minimum data transmit rate for associated clients. A radio continues to scan on its active data channel and on other channels and reports the results to its WSS switch.

Periodically, the switch examines these results to determine whether the channel or the power needs to be changed.

Power Tuning

By default, the switch evaluates the scan results for possible power changes every 300 seconds (5 minutes), and raises or lowers the default power level if needed.

A radio can temporarily increase its power level from the default at any time to correct either of the following client-related symptoms:

- Increase in the number of duplicate packets received from a client. This symptom indicates that the AP radio's acknowledgements (ACKs) are not reaching the client.
- Increase in the number of retransmissions of unicast packets from the radio to a client.

The radio uses two methods to treat these symptoms. First, if the data rate at which the radio is sending packets to the client is above the minimum data rate allowed, the radio lowers the unicast data rate with the client down to the next valid rate.

If the retransmissions still exceed the threshold, the radio continues to lower the data rate, one setting at a time, until either the retransmissions fall under the threshold or the minimum allowed data rate is reached.

If the retransmissions still exceed the threshold after the minimum allowed data rate is reached, the radio increases power by 1 dBm. The radio continues increasing the power in 1 dBm increments until the retransmissions fall to or below the threshold.

After the retransmissions fall to or below the threshold, the radio reduces power by 1 dBm. As long as retransmissions remain within the allowed threshold, the radio continues reducing power in 1 dBm increments until it returns to its default power level.

Channel Tuning

By default, the switch evaluates the scan results for possible channel changes every 3600 seconds (1 hour). WSS Software uses the following parameters to determine whether to change the channel on a radio:

- Received signal strength indication (RSSI)
- Amount of noise on the channel
- Packet retransmission count, which is the rate at which the radio receives retransmitted packets.
- Utilization, calculated based on the number of multicast packets per second that a radio can send on a channel while continuously sending fixed-size frames over a period of time.
- Phy error count, which is the number of frames received by the AP radio that have physical layer errors. A high number of Phy errors can indicate the presence of a non-802.11 device using the same RF spectrum.
- Received CRC error count. A high number of CRC errors can indicate a hidden node or co-channel interference.

The thresholds for these parameters are not configurable. RF Auto-Tuning also can change a radio's channel when the channel tuning interval expires, if a channel that has less disturbance is detected. *Disturbance* is based on the number of neighbors the radio has and each neighbor's RSSI.

A radio also can change its channel before the channel tuning interval expires to respond to RF anomalies. An RF anomaly is a sudden major change in the RF environment, such as sudden major interference on the channel.

By default, a radio cannot change its channel more often than every 900 seconds, regardless of the RF environment. This channel holddown avoids unnecessary changes due to very transient RF changes, such as activation of a microwave oven.

Tuning the Transmit Data Rate

A radio sends beacons, probe requests, and probe responses at the minimum transmit data rate allowed for clients. This gives them the maximum distance. All other packets are transmitted at a rate determined by their destination. All packets are transmitted at the same power level.

By default, the following minimum data rates are allowed:

- 5.5 Mbps for 802.11b/g clients
- 24 Mbps for 802.11a clients

As described in "Power Tuning" on page 293, a radio can lower the data rate with a client in order to improve the connection with that client.

RF Auto-Tuning Parameters

Table 19 lists the RF Auto-Tuning parameters and their default settings.

Table 19: Defaults for RF Auto-Tuning Parameters

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
Radio profile parameters		
channel-config	**enable**	When the radio is first enabled, RF Auto-Tuning sets the channel based on the channels in use on neighboring access ports.
channel-interval	**3600**	Every 3600 seconds, WSS Software examines the RF information gathered from the network and determines whether the channel needs to be changed to compensate for RF changes.
channel-holddown	**900**	WSS Software maintains the channel setting on a radio for at least 900 seconds regardless of RF changes.
power-config	**disable**	WSS Software uses the highest power level allowed for the country of operation or the highest supported by the hardware, whichever is lower.
power-interval	**300**	Every 300 seconds, WSS Software examines the RF information gathered from the network and determines whether the power needs to be changed to compensate for RF changes.
power-backoff-timer	**10**	If RF Auto-Tuning has increased power due to unacceptably high packet retransmissions or to maintain at least the minimum data rate for clients, and those conditions are no longer occurring, the radio reduces power by 1 dBm every 10 seconds, so long as the conditions do not recur.
Individual radio parameters		
max-power	Maximum allowed for country of operation	RF Auto-Tuning never sets a radio's power to a level that is higher than the maximum allowed for the country of operation (countrycode).

Table 19: Defaults for RF Auto-Tuning Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set To Default Value
max-retransmissions	**10**	If more than 10% of the packets received by the radio from a client are retransmissions, the radio lowers the data rate to the client and, if necessary, increases power to reduce the retransmissions.
min-client-rate	**5.5** for 802.11b/g **24** for 802.11a	The radio maintains a transmit rate of at least 5.5 Mbps for all 802.11b/g clients and 24 Mbps for all 802.11a clients.

Changing RF Auto-Tuning Settings

Changing Channel Tuning Settings

Disabling or Reenabling Channel Tuning

RF Auto-Tuning for channels is enabled by default. To disable or reenable the feature for all radios in a radio profile, use the following command:

set radio-profile *name* **auto-tune channel-config {enable | disable}**

To disable channel tuning for radios in the *rp2* radio profile, type the following command:

```
23x0# set radio-profile rp2 auto-tune channel-config disable
success: change accepted.
```

Changing the Channel Tuning Interval

The default channel tuning interval is 3600 seconds. You can change the interval to a value from 0 to 65535 seconds. If you set the interval to 0, RF Auto-Tuning does not reevaluate the channel at regular intervals. However, RF Auto-Tuning can still change the channel in response to RF anomalies. Nortel recommends that you use an interval of at least 300 seconds (5 minutes).

To change the channel tuning interval, use the following command:

set radio-profile *name* **auto-tune channel-interval** *seconds*

To set the channel tuning interval for radios in radio profile *rp2* to 2700 seconds (45 minutes), type the following command:

```
23x0# set radio-profile rp2 auto-tune channel-interval 2700
success: change accepted.
```

Changing the Channel Holddown Interval

The default channel holddown interval is 900 seconds. You can change the interval to a value from 0 to 65535 seconds. To change the channel holddown interval, use the following command:

set radio-profile *name* **auto-tune channel-holddown** *holddown*

To change the channel holddown for radios in radio profile *rp2* to 600 seconds, type the following command:

```
23x0# set radio-profile rp2 auto-tune channel-holddown 600
success: change accepted.
```

Changing Power Tuning Settings

Enabling Power Tuning

RF Auto-Tuning for power is disabled by default. To enable or disable the feature for all radios in a radio profile, use the following command:

set radio-profile *name* **auto-tune power-config {enable | disable}**

To enable power tuning for radios in the *rp2* radio profile, type the following command:

```
23x0# set radio-profile rp2 auto-tune power-config enable
success: change accepted.
```

Changing the Power Tuning Interval

The default power tuning interval is 300 seconds. You can change the interval to a value from 1 to 65535 seconds. To change the power tuning interval, use the following command:

set radio-profile *name* **auto-tune power-interval** *seconds*

To set the power tuning interval for radios in radio profile *rp2* to 240 seconds, type the following command:

```
23x0# set radio-profile rp2 auto-tune power-interval 240
success: change accepted.
```

Changing the Power Backoff Interval

The default power backoff interval is 10 seconds. You can change the interval to a value from 0 to 65535 seconds. To change the power backoff interval, use the following command:

set radio-profile *name* **auto-tune power-backoff-timer** *seconds*

To change the power-backoff interval for radios in radio profile *rp2* to 15 seconds, type the following command:

```
23x0# set radio-profile rp2 auto-tune power-backoff-timer 15
success: change accepted.
```

Changing the Maximum Default Power Allowed On a Radio

By default, the maximum default power level that RF Auto-Tuning can set on a radio is the same as the maximum power level allowed for the country of operation. To change the maximum default power level that RF Auto-Tuning can assign, use the following command:

set {ap *port-list* **| dap** *dap-num***} radio {1 | 2} auto-tune max-power** *power-level*

The *power-level* can be a value from 1 to 20.

To set the maximum power that RF Auto-Tuning can set on radio 1 on the AP access point on port 7 to 12 dBm, type the following command.

```
23x0# set ap 7 radio 1 auto-tune max-power 12
success: change accepted.
```

Changing the Client Retransmission Threshold

By default, the maximum percentage of client retransmissions a radio can experience before RF Auto-Tuning considers changing the channel on the radio is 10 percent. You can change the threshold to value from 1 to 100 percent. To change the max-retransmissions threshold, use the following command:

set {**ap** *port-list* | **dap** *dap-num*} **radio** {**1** | **2**} **auto-tune max-retransmissions** *retransmissions*

Examples To change the max-retransmissions threshold to 20 percent for radio 1 on the directly connected AP access point on port 7, type the following command:

```
23x0# set ap 7 radio 1 auto-tune max-retransmissions 20
success: change accepted.
```

Changing the Minimum Transmit Data Rate

By default, a radio does not lower the transmit data rate for any client below the following values:

- 5.5 Mbps for 802.11b/g clients
- 24 Mbps for 802.11a clients

To change the minimum transmit data rate for 802.11b/g clients or 802.11a clients, use the following command:

set {ap *port-list* **| dap** *dap-num***} radio {1 | 2} auto-tune min-client-rate** *rate*

The *rate* can be one of the following:

- For 802.11g radios—**54**, **48**, **36**, **24**, **18, 12**, **11**, **9**, **6**, **5.5**, **2**, or **1**
- For 802.11b radios—**11**, **5.5**, **2**, or **1**
- For 802.11a radios—**54**, **48**, **36**, **24**, **18**, **12**, **9**, or **6**

Displaying RF Auto-Tuning Information

You can display the RF Auto-Tuning configuration, a list of RF neighbors, and the values of RF attributes.

(For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

Displaying RF Auto-Tuning Settings

To display the RF Auto-Tuning settings that you can configure in a radio profile, use the following command:

show radio-profile {*name* | **?**}

Entering **show radio-profile ?** displays a list of radio profiles.

To display the RF Auto-Tuning and other settings in the *default* radio profile, type the following command:

```
23x0# show radio-profile default
Beacon Interval:            100   DTIM Interval:                    1
Max Tx Lifetime:           2000   Max Rx Lifetime:               2000
RTS Threshold:             2346   Frag Threshold:                2346
Short Retry Limit:            5   Long Retry Limit:                 5
Long Preamble:               NO   Allow 802.11g clients only:      NO
Tune Channel:               yes   Tune Power:                      no
Tune Channel Interval:     3600   Tune Power Interval:            600
Power Backoff Timer:         10   Channel Holddown:               300
Countermeasures:           none   Active-Scan:                    yes
WMM enabled:                yes
Service profiles: default-dot1x, default-clear
```

To display the RF Auto-Tuning settings that you can configure on an individual radio, use the following commands:

show ap config [*port-list* **[radio {1 | 2}]]**

show dap config [*dap-num* **[radio {1 | 2}]]**

To display the RF Auto-Tuning and other individual radio settings on radio 1 of a directly connected AP access point connected to WSS port 2, type the following command:

```
23x0# show ap config 2 radio 1
Port  2: AP model: AP-352, POE:  enable, bias: high, name: AP02
           boot-download-enable: YES
           load balancing group: none
  Radio 1: type: 802.11g, mode: disabled, channel:  6
  tx pwr:  1, profile: default
  auto-tune max-power: default, min-client-rate: 5.5, max-retransmissions: 10
```

To display the RF Auto-Tuning and other individual radio settings on both radios on the Distributed AP access point configured on connection 1, type the following command:

```
23x0# show dap config 1
Dap  1: serial-id:   12345678, AP model: AP-352, bias: high, name: DAP01
        fingerprint: b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
        boot-download-enable: YES
        load balancing group: none
  Radio 1: type: 802.11g, mode: disabled, channel:  6
  tx pwr:  1, profile: default
  auto-tune max-power: default, min-client-rate: 5.5, max-retransmissions: 10
  Radio 2: type: 802.11a, mode: disabled, channel: 36
  tx pwr:  1, profile: default
  auto-tune max-power: default, min-client-rate: 24, max-retransmissions: 10
```

Displaying RF Neighbors

To display the other radios that a specific Nortel radio can hear, use the following commands:

show auto-tune neighbors [ap *AP-num* **[radio {1 | 2| all}]]**

show auto-tune neighbors [dap *dap-num* **[radio {1 | 2| all}]]**

The list of radios includes beaconed third-party SSIDs, and both beaconed and unbeaconed Nortel SSIDs.

To display neighbor information for radio 1 on the directly connected AP access point on port 2, type the following command:

```
23x0# show auto-tune neighbors ap 2 radio 1
Total number of entries for port 2 radio 1: 5
Channel Neighbor BSS/MAC  RSSI
------- ----------------- ----
      1 00:0b:85:06:e3:60  -46
      1 00:0b:0e:00:0a:80  -78
      1 00:0b:0e:00:d2:c0  -74
      1 00:0b:85:06:dd:00  -50
      1 00:0b:0e:00:05:c1  -72
```

Displaying RF Attributes

To display the current values of the RF attributes RF Auto-Tuning uses to decide whether to change channel or power settings, use the following commands:

show auto-tune attributes [ap *AP-num* **[radio {1 | 2| all}]]**

show auto-tune attributes [dap *dap-num* **[radio {1 | 2| all}]]**

To display RF attribute information for radio 1 on the directly connected AP access point on port 2, type the following command:

```
23x0# show auto-tune attributes ap 2 radio 1
Auto-tune attributes for port 2 radio 1:
 Noise:                  -92 Packet Retransmission Count:          0
 Utilization:              0 Phy Errors Count:                     0
 CRC Errors count:       122
```

Wi-Fi Multimedia

How WMM Works in WSS Software 305
Disabling or Reenabling WMM 308
Displaying WMM Information 309

WSS Software supports Wi-Fi Multimedia (WMM). WMM provides wireless Quality of Service for time-sensitive applications such as voice and video. WMM is a pre-standard version of IEEE 802.11e, provided by the Wi-Fi Alliance to enable vendors to provide interoperable multimedia support before ratification of the standard.

WMM maps priority information between wired and wireless packets, so that high priority traffic receives end-to-end high priority treatment through the network.

WMM is enabled by default and does not require any configuration. You can disable the feature on individual radio profiles.

Note. WSS Software also can support non-WMM VoIP devices. However, to provide priority service to non-WMM VoIP traffic, you must configure an ACL to set the CoS for the traffic. The AP maps this CoS value to a forwarding queue. (For information, see "Enabling Prioritization for Legacy Voice over IP" on page 376.)

How WMM Works in WSS Software

WSS switches support WMM by tagging QoS information in packets. WSS Software classifies QoS information in a packet received by the switch. WSS Software then tags the packet's QoS information before forwarding the packet. Depending on the destination, WSS Software can set QoS information by setting a packet's 802.1p value or by setting the IP ToS value in the IP tunnel header, if the traffic is tunneled. WSS Software does not change the IP ToS value in the data packets themselves.

QoS on the WSS Switch

The WSS switch obtains an inbound packet's QoS value from the packet's Layer 2 802.1p or Layer 3 IP ToS value.

Depending on the destination, the switch maps the QoS information to other parts of the packet before forwarding it. If a packet has both 802.1p and IP ToS information, the switch sets QoS for the packet based on the IP ToS value.

However, if an ACL is mapped to the outbound traffic direction on the AP port, Distributed AP, or user VLAN, the switch sets QoS based on the CoS value in the ACL, regardless of the 802.1p and IP ToS values in the packet. (For information about using ACLs to change CoS, see "Using ACLs to Change CoS" on page 374.)

- If the WSS is forwarding a packet to an AP, WSS Software encapsulates the packet in an IP tunnel, and marks the IP ToS value in the tunnel header based on the incoming QoS value. This occurs for directly connected APs and for Distributed APs. The WSS never changes the data packet's IP ToS value.
- If the WSS is forwarding a packet through a tunnel to another WSS switch, WSS Software uses the same process used for traffic to an AP. Generally, an WSS switch uses a tunnel to send user data to another WSS switch when the user's VLAN is configured on the other switch but not on the local switch.
- If the WSS is forwarding a packet on a wired interface that has an 802.1Q VLAN tag, the switch sets the packet's 802.1p value based on the incoming QoS value.
- If the WSS is forwarding a packet to a non-tagged wired interface, and the traffic is not tunneled, the switch does not set the data packet's 802.1p value.

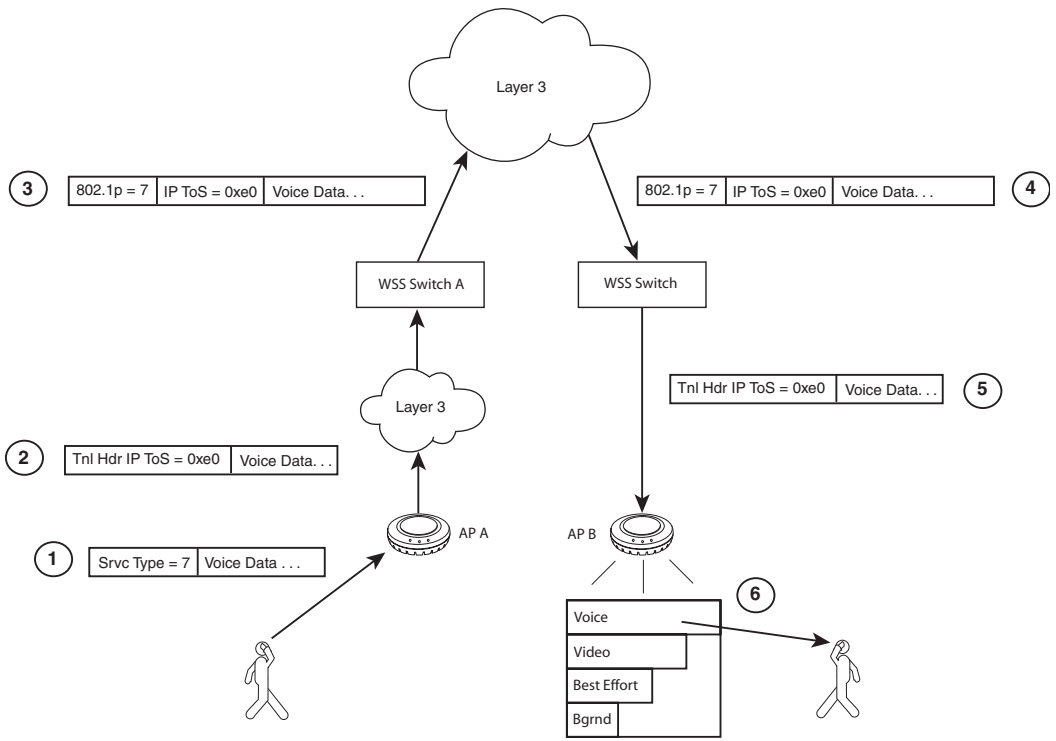
QoS on an AP

AP access ports use forwarding queues to prioritize traffic to wireless clients. When the AP receives a packet from an WSS switch, the AP places the packet into one of four forwarding queues. The AP's queue selection is based on the IP ToS setting in the tunnel header of the encapsulated data packet received from the WSS. The AP has the following forwarding queues, listed from lowest priority to highest priority:

- Background
- Best effort
- Video
- Voice

Figure 15 shows an example of WMM providing high priority forwarding for voice traffic through the network.

Figure 15. WMM in a Nortel Network



This figure shows the following process:

1 A user sends voice traffic from a WMM VoIP phone. The phone marks the QoS field of the packet with service type 7, indicating that the packet is for high priority (voice) traffic.

2 AP A receives the voice packet, encapsulates the data in an IP tunnel packet, and maps the service type to the equivalent IP ToS value in the tunnel header. Then the AP sends the packet to the WSS switch.

3. WSS A examines the 802.1p and IP ToS information in the packet. If the interface on which the switch will forward the packet is part of a tagged VLAN, the WSS switch maps the IP ToS value of the tunnel header to the 802.1p priority field of the data packet. The packet is now marked as high priority at Layer 2 as well as Layer 3.
4. The packet emerges from the network cloud between the WSS switches with the same priority information.
5. WSS B receives the packet, examines the 802.1p and IP ToS information in the packet, and encapsulates the data packet in a tunnel packet for sending to the AP. The switch sets the IP ToS value in the tunnel header based on the data packet's IP ToS value, or based on the 802.1p value if IP ToS is set to 0 in the data packet itself.

   If the packet matches a permit ACL mapped to the outbound traffic direction on the AP port, Distributed AP, or user VLAN, and the ACL sets the CoS value, the tunnel header's IP ToS value is set based on the CoS value in the ACL instead.

   WSS B sends the encapsulated data packet to AP B.
6. AP B receives the packet and maps the IP ToS value in the tunnel header to the Voice forwarding queue on the AP. The Voice queue has statistically more access to the air than the other queues, so the user's voice traffic receives priority treatment.

Table 20 shows how WMM priority information is mapped across the network. When WMM is enabled in WSS Software, Nortel switches and APs perform these mappings automatically.

Table 20: WMM Priority Mappings

Service Type	IP Precedence	IP ToS	DSCP	802.1p	CoS	AP Forwarding Queue
0	0	0	0	0	0	Background
3	3	0x60	24	3	3	
1	1	0x20	8	1	1	Best Effort
2	2	0x40	16	2	2	
4	4	0x80	32	4	4	Video
5	5	0xa0	40	5	5	
6	6	0xc0	48	6	6	Voice
7	7	0xe0	56	7	7	

Disabling or Reenabling WMM

WMM is enabled by default on all radio profiles. To disable the feature on a radio profile, use the following command:

set radio-profile *name* **wmm {enable | disable}**

When WMM is disabled, AP forwarding prioritization is optimized for SVP instead of WMM, and the AP does not tag packets it sends to the WSS. Otherwise, the classification and tagging described in "How WMM Works in WSS Software" on page 305 remain in effect.

If you plan to use SVP or another non-WMM type of prioritization, you must configure ACLs to tag the packets. (See "Enabling Prioritization for Legacy Voice over IP" on page 376.)

Displaying WMM Information

You can display the WMM state for a radio profile. You also can display statistics for AP forwarding queues.

Displaying the WMM State

To display the WMM state for a radio profile, use the following command:

show radio-profile {*name* | **?**}

The WMM state is displayed in the WMM enabled field.

```
23x0# show radio-profile radprof1
Beacon Interval:           100   DTIM Interval:                    1
Max Tx Lifetime:          2000   Max Rx Lifetime:               2000
RTS Threshold:            2346   Frag Threshold:                2346
Short Retry Limit:           5   Long Retry Limit:                 5
Long Preamble:              NO   Allow 802.11g clients only:      NO
Tune Channel:              yes   Tune Power:                      no
Tune Channel Interval:    3600   Tune Power Interval:            600
Power Backoff Timer:        10   Channel Holddown:               300
Countermeasures:          none   Active-Scan:                    yes
WMM enabled:                yes
Service profiles: srvcprof1
```

Displaying AP Forwarding Queue Statistics

You can display statistics for AP forwarding queues, using the following commands:

show dap qos-stats [*dap-num*]

show dap qos-stats [*port-list*]

The following command shows statistics for the AP forwarding queues on a Distributed AP:

```
23x0# show dap qos-stats 4

CoS   Queue      Tx
============================
    DAP: 4 radio: 1
1,2   Background         19
0,3   BestEffort        437
4,5   Video            3034
6,7   Voice            3068
```

```
CoS   Queue      Tx
============================
    DAP: 4 radio: 2
1,2   Background         11
0,3   BestEffort        221
4,5   Video             3631
6,7   Voice             7892
```

Configuring and Managing Spanning Tree Protocol

Enabling the Spanning Tree Protocol 312
Changing Standard Spanning Tree Parameters 313
Configuring and Managing STP Fast Convergence Features 319
Displaying Spanning Tree Information 326
Spanning Tree Configuration Scenario 332

The purpose of the Spanning Tree Protocol (STP) is to maintain a loop-free network. A loop-free path is accomplished when a device recognizes a loop in the topology and blocks one or more redundant paths.

Mobility System Software (WSS Software) supports 802.1D and Per-VLAN Spanning Tree protocol (PVST+).

- WSS Software uses 802.1D bridge protocol data units (BPDUs) on VLAN ports that are untagged. However, each VLAN still runs its own instance of STP, even if two or more VLANs contain untagged ports. To run a single instance of STP in 802.1D mode on the entire switch, configure all network ports as untagged members of the same VLAN.
- WSS Software uses PVST+ BPDUs on VLAN ports that are tagged. PVST+ BPDUs include tag information in the 802.1Q field of the BPDUs. WSS Software runs a separate instance of PVST+ on each tagged VLAN.

Note. STP does not run on AP access ports or wired authentication ports and does not affect traffic flow on these port types.

Note. When you create a VLAN, STP is disabled on the new VLAN by default, regardless of the STP state of other VLANs on the device.

Note. The IEEE 802.1D spanning tree specifications refer to networking devices that forward Layer 2 traffic as *bridges*. In this context, an WSS switch is a bridge. Where this manual or the product interface uses the term *bridge*, you can assume the term is applicable to the WSS switch.

Enabling the Spanning Tree Protocol

STP is disabled by default. You can enable STP globally or on individual VLANs.

To enable STP, use the following command:

set spantree {**enable** | **disable**}
[{**all** | **vlan** *vlan-id* | **port** *port-list vlan-id*}]

To enable STP on all VLANs configured on an WSS switch, type the following command:

```
23x0# set spantree enable
success: change accepted.
```

To verify the STP state and display the STP parameter settings, enter the **show spantree** command. For information, see "Displaying Spanning Tree Information" on page 326.

Changing Standard Spanning Tree Parameters

You can change the following standard STP parameters:

- Bridge priority
- Port cost
- Port priority

Bridge Priority

The bridge priority determines the WSS switch's eligibility to become the root bridge. You can set this parameter globally or on individual VLANs.

The root bridge is elected based on the bridge priority of each device in the spanning tree. The device with the highest bridge priority is elected to be the root bridge for the spanning tree. The bridge priority is a numeric value from 0 through 65,535. Lower numeric values represent higher priorities. The highest priority is 0, and the lowest priority is 65,535. The default bridge priority for all devices is 32,768.

If more than one device has the highest bridge priority (lowest numeric value), the device with the lowest MAC address becomes the root bridge.

If the root bridge fails, STP elects a new root bridge based on the bridge priorities of the remaining bridges.

Port Cost

Port cost is a numeric value that STP adds to the total cost of a path to the root bridge. When a designated bridge has multiple equal-cost paths to the root bridge, the designated bridge uses the path with the lowest total cost. You can set this parameter on an individual port basis, for all VLANs the port is in, or for specific VLANs.

You can specify a value from 1 through 65,535 for the port cost. The default depends on the port speed and link type. Table 21 lists the defaults for STP port path cost.

Table 21: SNMP Port Path Cost Defaults

Port Speed	Link Type	Default Port Path Cost
1000 Mbps	Full Duplex Aggregate Link (Port Group)	19
1000 Mbps	Full Duplex	4
100 Mbps	Full Duplex Aggregate Link (Port Group)	19
100 Mbps	Full Duplex	18
100 Mbps	Half Duplex	19
10 Mbps	Full Duplex Aggregate Link (Port Group)	19

Table 21: SNMP Port Path Cost Defaults (continued)

Port Speed	Link Type	Default Port Path Cost
10 Mbps	Full Duplex	95
10 Mbps	Half Duplex	100

Port Priority

Port priority is the eligibility of the port to be the designated port to the root bridge, and thus part of the path to the root bridge. When the WSS switch has more than one link to the root bridge, STP uses the link with the lowest priority value. You can set this parameter on an individual port basis, for all VLANs the port is in, or for specific VLANs.

Specify a priority from 0 (highest priority) through 255 (lowest priority). The default is 128.

Changing the Bridge Priority

To change the bridge priority, use the following command:

set spantree priority *value* {**all** | **vlan** *vlan-id*}

Specify a bridge priority from 0 through 65,535. The default is 32,768. The **all** option applies the change globally to all VLANs. Alternatively, specify an individual VLAN.

To change the bridge priority of VLAN *pink* to 69, type the following command:

```
23x0# set spantree priority 69 vlan pink
success: change accepted.
```

Changing STP Port Parameters

You can change the STP cost and priority of an individual port, on a global basis or an individual VLAN basis.

Changing the STP Port Cost

To change the cost of a port, use one of the following commands.

set spantree portcost *port-list* **cost** *cost*

set spantree portvlancost *port-list* **cost** *cost* {**all** | **vlan** *vlan-id*}

The **set spantree portcost** command changes the cost for ports in the default VLAN (VLAN 1) only. The **set spantree portvlancost** command changes the cost for ports in a specific other VLAN or in all VLANs.

Specify a value from 1 through 65,535 for the cost. The default depends on the port speed and link type. (See Table 21 on page 313.)

The **all** option applies the change to all VLANs. Alternatively, specify an individual VLAN.

To change the cost on ports 3 and 4 in the default VLAN to 20, type the following command:

```
23x0# set spantree portcost 3,4 cost 20
success: change accepted.
```

To change the cost for the same ports in VLAN *mauve*, type the following command:

```
23x0# set spantree portvlancost 3,4 cost 20 vlan mauve
success: change accepted.
```

Resetting the STP Port Cost to the Default Value

To reset the STP port cost to the default value, use one of the following commands:

clear spantree portcost *port-list*

clear spantree portvlancost *port-list* {**all** | **vlan** *vlan-id*}

The command applies only to the ports you specify. The port cost on other ports remains unchanged.

To reset the cost of ports 3 and 4 in the default VLAN to the default value, type the following command:

```
23x0# clear spantree portcost 3-4
success: change accepted.
```

To reset the cost of ports 3 and 4 for VLAN *beige*, type the following command:

```
23x0# clear spantree portvlancost 3-4 vlan beige
success: change accepted.
```

Changing the STP Port Priority

To change the priority of a port, use one of the following commands:

set spantree portpri *port-list* **priority** *value*

set spantree portvlanpri *port-list* **priority** *value* {**all** | **vlan** *vlan-id*}

The **set spantree portpri** command changes the priority for ports in the default VLAN (VLAN 1) only. The **set spantree portvlanpri** command changes the priority for ports in a specific other VLAN or in all VLANs.

Specify a priority from 0 (highest priority) through 255 (lowest priority). The default is 128.

The **all** option applies the change to all VLANs. Alternatively, specify an individual VLAN.

To set the priority of ports 3 and 4 in the default VLAN to 48, type the following command:

```
23x0# set spantree portpri 3-4 priority 48
success: change accepted.
```

To set the priority of ports 3 and 4 to 48 in VLAN *mauve*, type the following command:

```
23x0# set spantree portvlanpri 3-4 priority 48 vlan mauve
success: change accepted.
```

Resetting the STP Port Priority to the Default Value

To reset the STP port priority to the default value, use one of the following commands:

clear spantree portpri *port-list*

clear spantree portvlanpri *port-list* {**all** | **vlan** *vlan-id*}

The command applies only to the ports you specify. The port cost on other ports remains unchanged.

Changing Spanning Tree Timers

You can change the following STP timers:

- Hello interval—The interval between configuration messages sent by an WSS switch when the switch is acting as the root bridge. You can specify an interval from 1 through 10 seconds. The default is 2 seconds.
- Forwarding delay—The period of time a bridge other than the root bridge waits after receiving a topology change notification to begin forwarding data packets. You can specify a delay from 4 through 30 seconds. The default is 15 seconds. (The root bridge always forwards traffic.)
- Maximum age—The period of time that an WSS switch acting as a designated bridge waits for a new hello packet from the root bridge before determining that the root bridge is no longer available and initiating a topology change. You can specify an age from 6 through 40 seconds. The default is 20 seconds.

Changing the STP Hello Interval

To change the hello interval, use the following command:

set spantree hello *interval* {**all** | **vlan** *vlan-id*}

Specify an interval from 1 through 10 seconds. The default is 2 seconds.

The **all** option applies the change to all VLANs. Alternatively, specify an individual VLAN.

To change the hello interval for all VLANs to 4 seconds, type the following command:

```
23x0# set spantree hello 4 all
success: change accepted.
```

Changing the STP Forwarding Delay

To change the forwarding delay, use the following command:

set spantree fwddelay *delay* {**all** | **vlan** *vlan-id*}

Specify a delay from 4 through 30 seconds. The default is 15 seconds.

The **all** option applies the change to all VLANs. Alternatively, specify an individual VLAN.

To change the forwarding delay on VLAN *pink* to 20 seconds, type the following command:

```
23x0# set spantree fwddelay 20 vlan pink
success: change accepted.
```

Changing the STP Maximum Age

To change the maximum age, use the following command:

set spantree maxage *aging-time* {**all** | **vlan** *vlan-id*}

Specify an age from 6 through 40 seconds. The default is 20 seconds.

The **all** option applies the change to all VLANs. Alternatively, specify an individual VLAN.

To change the maximum acceptable age for root bridge hello packets on all VLANs to 15 seconds, type the following command:

```
23x0# set spantree maxage 15 all
success: change accepted.
```

Configuring and Managing STP Fast Convergence Features

The standard STP timers delay traffic forwarding briefly after a topology change. The time a port takes to change from the listening state to the learning state or from the learning state to the forwarding state is called the forwarding delay. In some configurations, this delay is unnecessary. The WSS switch provides the following fast convergence features to bypass the forwarding delay:

- Port fast
- Backbone fast
- Uplink fast

Port Fast Convergence

Port fast convergence bypasses both the listening and learning stages and immediately places a port in the forwarding state. You can use port fast convergence on ports that are directly connected to servers, hosts, or other MAC stations.

Note. Do not use port fast convergence on ports connected to other bridges.

Backbone Fast Convergence

Backbone fast convergence accelerates a port's recovery following the failure of an indirect link. Normally, when a forwarding link fails, a bridge that is not directly connected to the link does not detect the link change until the maximum age timer expires. Backbone fast convergence enables the WSS switch to listen for bridge protocol data units (BPDUs) sent by a designated bridge when the designated bridge's link to the root bridge fails. The switch immediately verifies whether BPDU information stored on a port is still valid. If not, the bridge immediately starts the listening stage on the port.

Note. If you plan to use the backbone fast convergence feature, you must enable it on all the bridges in the spanning tree.

Uplink Fast Convergence

Uplink fast convergence enables an WSS switch that has redundant links to the network core to immediately change the state of a backup link to forwarding if the primary link to the root fails. Uplink fast convergence bypasses the listening and learning states to immediately enter the forwarding state.



Note. The uplink fast convergence feature is applicable to bridges that are acting as access switches to the network core (distribution layer) but are not in the core themselves. Do not enable the feature on WSS switches that are in the network core.

Configuring Port Fast Convergence

To enable or disable port fast convergence, use the following command:

set spantree portfast port *port-list* **{enable | disable}**

To enable port fast convergence on ports 9, 11, and 13, type the following command:

```
23x0# set spantree portfast port 9,11,13 enable
success: change accepted.
```

Displaying Port Fast Convergence Information

To display port fast convergence information, use the following command:

show spantree portfast [*port-list*]

To display port fast convergence information for all ports, type the following command:

```
23x0# show spantree portfast
Port                        Vlan   Portfast
--------------------------- ----   ----------
1                           1      disable
2                           1      disable
3                           1      disable
4                           1      enable
5                           1      disable
6                           1      disable
7                           1      disable
8                           1      disable
10                          1      disable
15                          1      disable
16                          1      disable
17                          1      disable
18                          1      disable
19                          1      disable
20                          1      disable
21                          1      disable
22                          1      disable
11                          2      enable
12                          2      disable
13                          2      disable
14                          2      enable
```

In this example, port fast convergence is enabled on ports 11 and 14 in VLAN 2 and port 4 in VLAN 1.

Configuring Backbone Fast Convergence

To enable or disable backbone fast convergence, use the following command:

set spantree backbonefast {enable | disable}

To enable backbone fast convergence on all VLANs, type the following command:

```
23x0# set spantree backbonefast enable
success: change accepted.
```

Displaying the Backbone Fast Convergence State

To display the state of the backbone fast convergence feature, use the following command:

show spantree backbonefast

Here is an example:

```
23x0# show spantree backbonefast


  Backbonefast is enabled
```

In this example, backbone fast convergence is enabled.

Configuring Uplink Fast Convergence

To enable or disable uplink fast convergence, use the following command:

set spantree uplinkfast {enable | disable}

Displaying Uplink Fast Convergence Information

To display uplink fast convergence information, use the following command:

show spantree uplinkfast [**vlan** *vlan-id*]

The following command displays uplink fast convergence information for all VLANs:

```
23x0# show spantree uplinkfast
 VLAN     port     list
--------------------------------------------------------------------------------
1        1(fwd),2,3
```

In this example, ports 1, 2, and 3 provide redundant links to the network core. Port 1 is forwarding traffic. The remaining ports block traffic to prevent a loop.

Displaying Spanning Tree Information

You can use CLI commands to display the following STP information:

- Bridge STP settings and individual port information
- Blocked ports
- Statistics
- Port fast, backbone fast, and uplink fast convergence information



Note. For information about the **show** commands for the fast convergence features, see "Configuring and Managing STP Fast Convergence Features" on page 319.

Displaying STP Bridge and Port Information

To display STP bridge and port information, use the following command:

show spantree [*port-list* | **vlan** *vlan-id*] [**active**]

By default, STP information for all ports and all VLANs is displayed. To display STP information for specific ports or a specific VLAN only, enter a port list or a VLAN name or number. For each VLAN, only the ports contained in the VLAN are listed in the command output.

To list only the ports that are in the active (forwarding) state, enter the **active** option.

To display STP information for VLAN *mauve*, type the following command:

```
23x0# show spantree vlan mauve
VLAN     3
Spanning tree mode           PVST+
Spanning tree type           IEEE
Spanning tree enabled

Designated Root              00-02-4a-70-49-f7
Designated Root Priority     32768
Designated Root Path Cost    19
Designated Root Port         1
Root Max Age   20 sec   Hello Time 2 sec   Forward Delay 15 sec
Bridge ID MAC ADDR           00-0b-0e-02-76-f7
Bridge ID Priority           32768
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port               Vlan       Port-State    Cost   Prio   Portfast
-------------------------------------------------------------------------
1                   1        Forwarding      19   128     Disabled
2                   1        Blocking        19   128     Disabled
3                   1        Blocking        19   128     Disabled
10                  1        Forwarding      19   128     Disabled
15                  1        Blocking        19   128     Disabled
16                  1        Blocking        19   128     Disabled
```

In this example, VLAN *mauve* contains ports 1 through 3, 10, 15 and 16. Ports 1 and 10 are forwarding traffic. The other ports are blocking traffic.

(For more information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

Displaying the STP Port Cost on a VLAN Basis

To display a brief list of the STP port cost for a port in each of its VLANs, use the following command:

show spantree portvlancost *port-list*

This command displays the same information as the **show spantree** command's Cost field in a concise format for all VLANs. The **show spantree** command lists all the STP information separately for each VLAN.

To display the STP port cost of port 1, type the following command:

```
23x0# show spantree portvlancost 1
port 1 VLAN 1 have path cost 19
```

Displaying Blocked STP Ports

To display information about ports that are in the STP blocking state, use the following command:

show spantree blockedports [**vlan** *vlan-id*]

To display information about blocked ports on an WSS switch for the *default* VLAN (VLAN 1), type the following command:

23x0# show spantree blockedports vlan default

```
Port            Vlan      Port-State    Cost   Prio   Portfast
-------------------------------------------------------------------
22               190       Blocking        4   128    Disabled

Number of blocked ports (segments) in VLAN 1 : 1
```

(For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

Displaying Spanning Tree Statistics

To display STP statistics, use the following command:

show spantree statistics [*port-list* [**vlan** *vlan-id*]]

To display STP statistics for port 1, type the following command:

```
23x0# show spantree statistics 1

BPDU related parameters


Port 1                      VLAN 1
spanning tree enabled for VLAN = 1
port spanning tree                          enabled
state                                       Forwarding
port_id                                     0x8015
port_number                                 0x15
path cost                                   0x4
message age (port/VLAN)                     0(20)
designated_root                             00-0b-0e-00-04-30
designated cost                             0x0
designated_bridge                           00-0b-0e-00-04-30
designated_port                             38
top_change_ack                              FALSE
config_pending                              FALSE
port_inconsistency                          none


              Port based information statistics

config BPDU's xmitted(port/VLAN)            0 (1)
config BPDU's received(port/VLAN)           21825 (43649)
tcn BPDU's xmitted(port/VLAN)               0 (0)
tcn BPDU's received(port/VLAN)              2 (2)
forward transition count (port/VLAN)        1 (1)
scp failure count                           0
root inc trans count (port/VLAN)            1 (1)
inhibit loopguard                           FALSE
loop inc trans count                        0 (0)


            Status of Port Timers

forward delay timer                         INACTIVE
forward delay timer value                   15
message age timer                           ACTIVE
message age timer value                     0
```

```
topology change timer                    INACTIVE
topology change timer value              0
hold timer                               INACTIVE
hold timer value                         0
delay root port timer                    INACTIVE
delay root port timer value              0
delay root port timer restarted is       FALSE


             VLAN based information & statistics

spanning tree type                       ieee
spanning tree multicast address          01-00-0c-cc-cc-cd
bridge priority                          32768
bridge MAC address                       00-0b-0e-12-34-56
bridge hello time                        2
bridge forward delay                     15
topology change initiator:               0
last topology change occurred:           Tue Jul 01 2003 22:33:36.
topology change                          FALSE
topology change time                     35
topology change detected                 FALSE
topology change count                    1
topology change last recvd. from         00-0b-0e-02-76-f6


             Other port specific info

dynamic max age transition               0
port BPDU ok count                       21825
msg age expiry count                     0
link loading                             0
BPDU in processing                       FALSE
num of similar BPDU's to process         0
received_inferior_bpdu                   FALSE
next state                               0
src MAC count                            21807
total src MAC count                      21825
curr_src_mac                             00-0b-0e-00-04-30
next_src_mac                             00-0b-0e-02-76-f6
```

(For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

Clearing STP Statistics

To clear the STP statistics counters, use the following command.

clear spantree statistics *port-list* [**vlan** *vlan-id*]

As soon as you enter the command, WSS Software resets the STP counters for the specified ports or VLANs to 0. The software then begins incrementing the counters again.

Spanning Tree Configuration Scenario

This scenario configures a VLAN named *backbone* for an WSS switch's connections to the network backbone, adds ports 21 and 22 to the VLAN, and enables STP on the VLAN to prevent loops.

1. Remove the network cables from ports 21 and 22 or use WSS Software to disable the ports,. This prevents a loop until you complete the STP configuration. To disable the ports and verify the results, type the following commands:

```
23x0# set port disable 21-22
success: set "disable" on port 21-22
```

```
23x0# show port status
Port  Name              Admin  Oper    Config    Actual    Type       Media
================================================================================
   1                    up     up      auto      100/full  network    10/100BaseTx
   2                    up     down    auto                network    10/100BaseTx
   3                    up     down    auto                network    10/100BaseTx
   4                    up     down    auto                network    10/100BaseTx
   5                    up     down    auto                network    10/100BaseTx
   6                    up     down    auto                network    10/100BaseTx
   7                    up     down    auto                network    10/100BaseTx
   8                    up     down    auto                network    10/100BaseTx
   9                    up     down    auto                network    10/100BaseTx
  10                    up     down    auto                network    10/100BaseTx
  11                    up     down    auto                network    10/100BaseTx
  12                    up     down    auto                network    10/100BaseTx
  13                    up     down    auto                network    10/100BaseTx
  14                    up     down    auto                network    10/100BaseTx
  15                    up     down    auto                network    10/100BaseTx
  16                    up     down    auto                network    10/100BaseTx
  17                    up     down    auto                network    10/100BaseTx
  18                    up     down    auto                network    10/100BaseTx
  19                    up     down    auto                network    10/100BaseTx
  20                    up     down    auto                network    10/100BaseTx
  21                  down     down    auto                network
  22                  down     down    auto                network
```

2. Configure a *backbone* VLAN and verify the configuration change. Type the following commands:

```
23x0# set vlan 10 name backbone port 21-22
success: change accepted.
```

```
23x0# show vlan config
                          Admin  VLAN  Tunl                          Port
VLAN Name                 Status State Affin Port            Tag    State
```

```
---- --------------- ------ ----- ----- --------------- ----- -----
   1 default         Up     Up        5
                                        1               none  Up
  10 backbone        Up     Down      5
                                       21               none  Down
                                       22               none  Down
```

3 Enable STP on the *backbone* VLAN and verify the change. Type the following commands:

```
23x0# set spantree enable vlan backbone
success: change accepted.

23x0# show spantree vlan 10

VLAN    10
Spanning tree mode           PVST+
Spanning tree type           IEEE
Spanning tree enabled

Designated Root              00-0b-0e-00-04-0c
Designated Root Priority     32768
Designated Root Path Cost    0
We are the root
Root Max Age   20 sec   Hello Time 2 sec   Forward Delay 15 sec
Bridge ID MAC ADDR           00-0b-0e-00-04-0c
Bridge ID Priority           32768
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port              Vlan       Port-State    Cost   Prio   Portfast
-----------------------------------------------------------------
-----
21                 10        Disabled         4   128     Disabled
22                 10        Disabled         4   128     Disabled
```

4 Reconnect or reenable ports 21 and 22 and verify the change. Type the following commands:

```
23x0# set port enable 21-22
success: set "enable" on port 21-22

23x0# show port status
Port  Name              Admin  Oper    Config    Actual    Type       Media
================================================================================
   1                    up     up      auto      100/full  network    10/100BaseTx
   2                    up     down    auto                network    10/100BaseTx
   3                    up     down    auto                network    10/100BaseTx
   4                    up     down    auto                network    10/100BaseTx
   5                    up     down    auto                network    10/100BaseTx
   6                    up     down    auto                network    10/100BaseTx
   7                    up     down    auto                network    10/100BaseTx
   8                    up     down    auto                network    10/100BaseTx
   9                    up     down    auto                network    10/100BaseTx
  10                    up     down    auto                network    10/100BaseTx
  11                    up     down    auto                network    10/100BaseTx
  12                    up     down    auto                network    10/100BaseTx
```

```
13                 up     down    auto                 network    10/100BaseTx
14                 up     down    auto                 network    10/100BaseTx
15                 up     down    auto                 network    10/100BaseTx
16                 up     down    auto                 network    10/100BaseTx
17                 up     down    auto                 network    10/100BaseTx
18                 up     down    auto                 network    10/100BaseTx
19                 up     down    auto                 network    10/100BaseTx
20                 up     down    auto                 network    10/100BaseTx
21                 up     up      auto      1000/full  network
22                 up     up      auto      1000/full  network
```

5 Wait for STP to complete the listening and learning stages and converge, then verify that STP is operating properly and blocking one of the ports in the *backbone* VLAN. Type the following command:

```
23x0# show spantree vlan 10

VLAN    10
Spanning tree mode           PVST+
Spanning tree type           IEEE
Spanning tree enabled

Designated Root              00-0b-0e-00-04-0c
Designated Root Priority     32768
Designated Root Path Cost    0
We are the root
Root Max Age   20 sec   Hello Time 2 sec   Forward Delay 15 sec
Bridge ID MAC ADDR           00-0b-0e-00-04-0c
Bridge ID Priority           32768
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port              Vlan      Port-State    Cost   Prio   Portfast
-----------------------------------------------------------------
-----
21                  10       Forwarding       4   128
Disabled
22                  10       Blocking         4   128
Disabled
```

6 Save the configuration. Type the following command:

```
23x0# save config
success: configuration saved.
```

Configuring and Managing IGMP Snooping

Disabling or Reenabling IGMP Snooping 335
Disabling or Reenabling Proxy Reporting 335
Enabling the Pseudo-Querier 336
Changing IGMP Timers 336
Enabling Router Solicitation 341
Configuring Static Multicast Ports 342
Displaying Multicast Information 344

Internet Group Management Protocol (IGMP) snooping controls multicast traffic on an WSS switch by forwarding packets for a multicast group only on the ports that are connected to members of the group. A multicast group is a set of IP hosts that receive traffic addressed to a specific Class D IP address, the group address.

The WSS switch listens for multicast packets and maintains a table of multicast groups, as well as their sources and receivers, based on the traffic. IGMP snooping is enabled by default.

You can configure IGMP snooping parameters and enable or disable the feature on an individual VLAN basis.

The current software version supports IGMP versions 1 and 2.

Disabling or Reenabling IGMP Snooping

IGMP snooping is enabled by default. To disable or reenable the feature, use the following command:

set igmp {**enable** | **disable**} [**vlan** *vlan-id*]

If you do not specify a VLAN ID, the change is applied to all VLANs on the WSS switch.

Disabling or Reenabling Proxy Reporting

Proxy reporting reduces multicast overhead by sending only one report for each active group to the multicast routers, instead of sending a separate report from each multicast receiver. For example, if the WSS switch receives reports from three receivers for multicast group 237.255.255.255, the switch sends only one report for the group to the routers. One report is sufficient to cause the routers to continue sending data for the group. Proxy reporting is enabled by default.

To disable or reenable proxy reporting, use the following command:

set igmp proxy-report {**enable** | **disable**} [**vlan** *vlan-id*]

Enabling the Pseudo-Querier

The IGMP pseudo-querier enables IGMP snooping to operate in a VLAN that does not have a multicast router to send IGMP general queries to clients.

Note. Nortel recommends that you use the pseudo-querier only when the VLAN contains local multicast traffic sources and no multicast router is servicing the subnet.

To enable the pseudo-querier, use the following command:

set igmp querier {**enable** | **disable**} [**vlan** *vlan-id*]

Changing IGMP Timers

You can change the following IGMP timers:

- Query interval—Number of seconds that elapse between general queries sent by the WSS switch to advertise multicast groups.
- Other-querier-present interval—Number of seconds that the WSS switch waits for a general query to arrive from another querier before electing itself the querier.
- Query response interval—Number of tenths of a second that the WSS switch waits for a receiver to respond to a group-specific query message before removing the receiver from the receiver list for the group.

Note. The query interval, other-querier-present interval, and query response interval are applicable only when the WSS switch is querier for the subnet. For the switch to become the querier, the pseudo-querier feature must be enabled on the switch and the switch must have the lowest IP address among all the devices eligible to become a querier. To enable the pseudo-querier feature, see "Enabling the Pseudo-Querier" on page 336.

- Last member query interval—Number of tenths of a second that the WSS switch waits for a response to a group-specific query after receiving a leave message for that group, before removing the receiver that sent the leave message from the list of receivers for the group. If there are no more receivers for the group, the switch also sends a leave message for the group to multicast routers.
- Robustness value—Number used as a multiplier to adjust the IGMP timers to the amount of traffic loss that occurs on the network. Set the robustness value higher to adjust for more traffic loss.

Changing the Query Interval

To change the IGMP query interval timer, use the following command:

set igmp qi *seconds* [**vlan** *vlan-id*]

For *seconds*, you can specify a value from 1 through 65,535. The default is 125 seconds.

Changing the Other-Querier-Present Interval

To change the other-querier-present interval, use the following command:

set igmp oqi *seconds* [**vlan** *vlan-id*]

For *seconds*, you can specify a value from 1 through 65,535. The default is 255 seconds.

Changing the Query Response Interval

To set the query response interval, use the following command:

set igmp qri *tenth-seconds* [**vlan** *vlan-id*]

You can specify a value from 1 through 65,535 tenths of a second. The default is 100 tenths of a second (10 seconds).

Changing the Last Member Query Interval

To set the last member query interval, use the following command:

set igmp lmqi *tenth-seconds* [**vlan** *vlan-id*]

You can specify a value from 1 through 65,535 tenths of a second. The default is 10 tenths of a second (1 second).

Changing Robustness

Robustness adjusts the IGMP timers to the amount of traffic loss that occurs on the network. Set the robustness value higher to adjust for more traffic loss. To change the robustness value, use the following command:

set igmp rv *num* [**vlan** *vlan-id*]

You can specify a value from 2 through 255. The default is 2.

Enabling Router Solicitation

An WSS switch can search for multicast routers by sending multicast router solicitation messages. This message invites multicast routers that receive the message and that support router solicitation to immediately advertise themselves to the WSS switch. Router solicitation is disabled by default.

The WSS Software implementation of router solicitation is based on *draft-ietf-idmr-igmp-mrdisc-09.txt*.

To enable or disable multicast router solicitation, use the following command:

set igmp mrsol {**enable** | **disable**} [**vlan** *vlan-id*]

Changing the Router Solicitation Interval

The default multicast router solicitation interval is 30 seconds. To change the interval, use the following command:

set igmp mrsol mrsi *seconds* [**vlan** *vlan-id*]

You can specify 1 through 65,535 seconds. The default is 30 seconds.

Configuring Static Multicast Ports

An WSS switch learns about multicast routers and receivers from multicast traffic it receives from those devices. When the WSS switch receives traffic from a multicast router or receiver, the switch adds the port that received the traffic as a multicast router or receiver port. The WSS switch forwards traffic to multicast routers only on the multicast router ports and forwards traffic to multicast receivers only on the multicast receiver ports.

The router and receiver ports that the WSS switch learns based on multicast traffic age out if they are unused.

You can add network ports as static multicast router ports or multicast receiver ports. Ports you add do not age out.



Note. You cannot add AP access ports or wired authentication ports as static multicast ports. However, WSS Software can dynamically add these port types to the list of multicast ports based on multicast traffic.

Adding or Removing a Static Multicast Router Port

To add or remove a static multicast router port, use the following command:

set igmp mrouter port *port-list* **enable** | **disable**

Adding or Removing a Static Multicast Receiver Port

To add a static multicast receiver port, use the following command:

set igmp receiver port *port-list* **enable** | **disable**

Displaying Multicast Information

You can use the CLI to display the following IGMP snooping information:

- Multicast configuration information and statistics
- Multicast queriers
- Multicast routers
- Multicast receivers

Displaying Multicast Configuration Information and Statistics

To display multicast configuration information and statistics, use the following command:

show igmp [**vlan** *vlan-id*]

The **show igmp** command displays the IGMP snooping state, the settings of all multicast parameters you can configure, and multicast statistics.

To display multicast information for VLAN *orange*, type the following command:

```
23x0# show igmp vlan orange
VLAN: orange
IGMP is enabled
Proxy reporting is on
Mrouter solicitation is on
Querier functionality is off
Configuration values: qi: 125 oqi: 300 qri: 100 lmqi: 10 rvalue: 2 Multicast
router information:
Port Mrouter-IPaddr Mrouter-MAC        Type  TTL
---- --------------- ----------------- ----- -----
  10      192.28.7.5 00:01:02:03:04:05 dvmrp    17
Group           Port Receiver-IP     Receiver-MAC      TTL
--------------- ---- --------------- ----------------- -----
      224.0.0.2 none            none               none undef
237.255.255.255    5     10.10.10.11 00:02:04:06:08:0b   258
237.255.255.255    5     10.10.10.13 00:02:04:06:08:0d   258
237.255.255.255    5     10.10.10.14 00:02:04:06:08:0e   258
237.255.255.255    5     10.10.10.12 00:02:04:06:08:0c   258
237.255.255.255    5     10.10.10.10 00:02:04:06:08:0a   258
Querier information:
Querier for vlan orange
Port Querier-IP      Querier-MAC       TTL
---- --------------- ----------------- -----
   1 193.122.135.178 00:0b:cc:d2:e9:b4    23
IGMP vlan member ports: 10, 12, 11, 14, 16, 15, 13, 18, 17, 1, 20, 21, 2,
22, 19, 4, 6, 5, 3, 8, 7, 9
IGMP static ports: none
IGMP statistics for vlan orange:

IGMP message type Received Transmitted Dropped
----------------- -------- ----------- -------
General-Queries          0           0       0
GS-Queries               0           0       0
Report V1                0           0       0
Report V2                5           1       4
Leave                    0           0       0
Mrouter-Adv              0           0       0
Mrouter-Term             0           0       0
Mrouter-Sol             50         101       0
```

```
DVMRP                    4           4       0
PIM V1                   0           0       0
PIM V2                   0           0       0
Topology notifications: 0
Packets with unknown IGMP type: 0
Packets with bad length: 0
Packets with bad checksum: 0
Packets dropped: 4
```

(For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

Displaying Multicast Statistics Only

To display multicast statistics only without also displaying all the other multicast information, use the following command:

show igmp statistics [vlan *vlan-id*]

Clearing Multicast Statistics

To clear the multicast statistics counters, use the following command:

clear igmp statistics [vlan *vlan-id*]

The counters begin incrementing again, starting from 0.

Displaying Multicast Queriers

To display information about the multicast querier only without also displaying all the other multicast information, use the following command:

show igmp querier [vlan *vlan-id*]

To display querier information for VLAN *orange*, type the following command:

```
23x0# show igmp querier vlan orange
Querier for vlan orange
Port Querier-IP      Querier-MAC       TTL
---- --------------- ----------------- -----
   1 193.122.135.178 00:0b:cc:d2:e9:b4    23
```

In this example, the pseudo-querier feature is enabled on VLAN orange.

(For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

Displaying Multicast Routers

To display information about the multicast routers only without also displaying all the other multicast information, use the following command:

show igmp mrouter [vlan *vlan-id*]

To display the multicast routers in VLAN *orange*, type the following command:

```
23x0# show igmp mrouter vlan orange
Multicast routers for vlan orange
Port Mrouter-IPaddr  Mrouter-MAC       Type  TTL
---- --------------- ----------------- ----- -----
  10      192.28.7.5 00:01:02:03:04:05 dvmrp    33
```

(For information about the fields in this display, see the *Nortel Mobility System Software Command Reference*.)

Displaying Multicast Receivers

To display information about the multicast receivers only without also displaying all the other multicast information, use the following command:

show igmp receiver-table [**vlan** *vlan-id*]
[**group** *group-ip-addr/mask-length*]

Use the **group** parameter to display receivers for a specific group or set of groups. For example, to display receivers for multicast groups 237.255.255.1 through 237.255.255.255, in all VLANs, type the following command:

```
23x0# show igmp receiver-table group 237.255.255.0/24
VLAN: red
Session         Port Receiver-IP     Receiver-MAC      TTL
--------------- ---- --------------- ----------------- -----
237.255.255.2      2     10.10.20.19 00:02:04:06:09:0d   112
237.255.255.119    3     10.10.30.31 00:02:04:06:01:0b   112

VLAN: green
Session         Port Receiver-IP     Receiver-MAC      TTL
--------------- ---- --------------- ----------------- -----
237.255.255.17    11     10.10.40.41 00:02:06:08:02:0c    12
237.255.255.255    6     10.10.60.61 00:05:09:0c:0a:01   111
```

(For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

Configuring and Managing Security ACLs

About Security Access Control Lists 351
Creating and Committing a Security ACL 353
Mapping Security ACLs 365
Modifying a Security ACL 369
Using ACLs to Change CoS 374
Enabling Prioritization for Legacy Voice over IP 376
Security ACL Configuration Scenario 377

About Security Access Control Lists

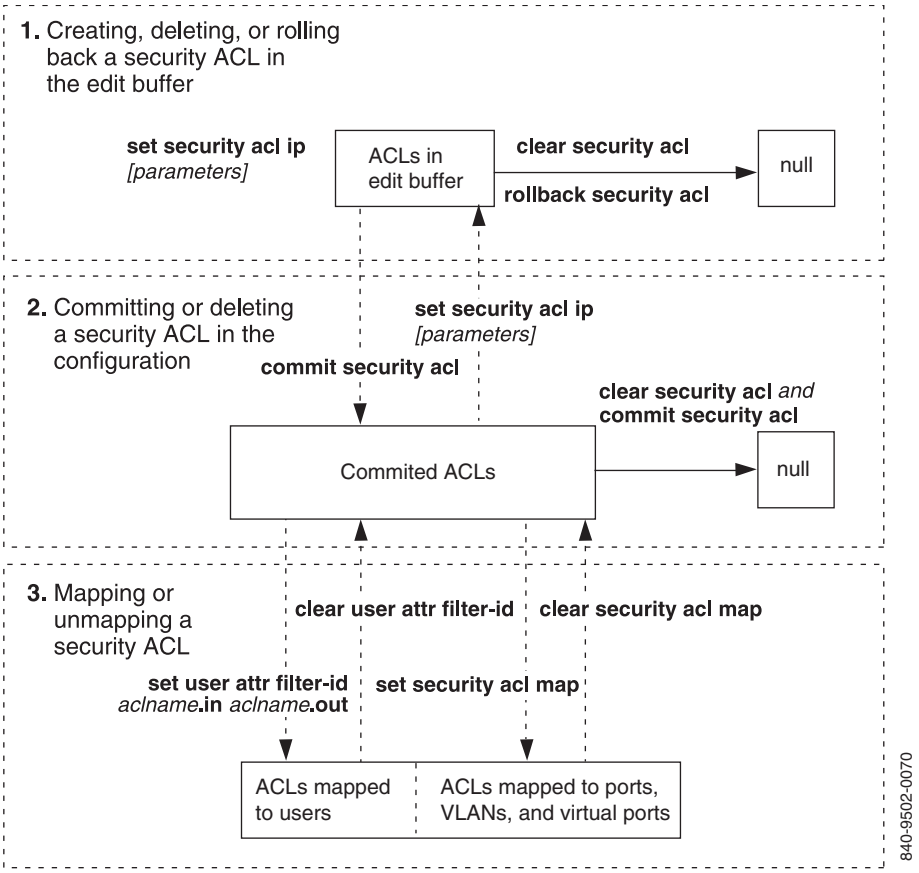
A security access control list (ACL) filters packets for the purpose of discarding them, permitting them, or permitting them with modification (marking) for class-of-service (CoS) priority treatment. A typical use of security ACLs is to enable users to send and receive packets within the local intranet, but restrict incoming packets to the server in which confidential salary information is stored.

Nortel provides a very powerful mapping application for security ACLs. In addition to being assigned to physical ports, VLANs, virtual ports in a VLAN, or Distributed APs, ACLs can be mapped dynamically to a user's session, based on authorization information passed back from the AAA server during the user authentication process.

Overview of Security ACL Commands

Figure 16 provides a visual overview of the way you use WSS Software commands to set a security ACL, commit the ACL so it is stored in the configuration, and map the ACL to a user session, VLAN, port, virtual port, or Distributed AP.

Figure 16: Setting Security ACLs


1. Creating, deleting, or rolling back a security ACL in the edit buffer
set security acl ip [parameters]
ACLs in edit buffer
clear security acl
rollback security acl
null
2. Committing or deleting a security ACL in the configuration
set security acl ip [parameters]
commit security acl
clear security acl and commit security acl
Commited ACLs
null
3. Mapping or unmapping a security ACL
clear user attr filter-id
clear security acl map
set user attr filter-id aclname.in aclname.out
set security acl map
ACLs mapped to users
ACLs mapped to ports, VLANs, and virtual ports
840-9502-0070

Security ACL Filters

A security ACL filters packets to restrict or permit network traffic. These filters can then be mapped by name to authenticated users, ports, VLANs, virtual ports, or Distributed APs. You can also assign a class-of-service (CoS) level that marks the packets matching the filter for priority handling.

A security ACL contains an ordered list of rules called access control entries (ACEs), which specify how to handle packets. An ACE contains an action that can deny the traffic, permit the traffic, or permit the traffic and apply to it a specific CoS level of packet handling. The filter can include source and destination IP address information along with other Layer 3 and Layer 4 parameters. Action is taken only if the packet matches the filter.

The order in which ACEs are listed in an ACL is important. WSS Software applies ACEs that are higher in the list before ACEs lower in the list. (See "Modifying a Security ACL" on page 369.) An implicit "deny all" rule is always processed as the last ACE of an ACL. If a packet matches no ACE in the entire mapped ACL, the packet is rejected. If the ACL does not contain at least one ACE that permits access, no traffic is allowed.

Plan your security ACL maps to ports, VLANs, virtual ports, and Distributed APs so that only one security ACL filters a given flow of packets. If more than one security ACL filters the same traffic, WSS Software applies only the first ACL match and ignores any other matches. Security ACLs that are mapped to users have precedence over ACLs mapped to ports, VLANs, virtual ports, or Distributed APs.

You cannot perform ACL functions that include permitting, denying, or marking with a Class of Service (CoS) level on packets with a multicast or broadcast destination address.

Creating and Committing a Security ACL

The security ACLs you create can filter packets by source address, IP protocol, port type, and other characteristics. When you configure an ACE for a security ACL, WSS Software stores the ACE in the edit buffer until you commit the ACL to be saved to the permanent configuration. You must commit a security ACL before you can apply it to an authenticated user's session or map it to a port, VLAN, virtual port, or Distributed AP. Every security ACL must have a name.

Setting a Source IP ACL

You can create an ACE that filters packets based on the source IP address and optionally applies CoS packet handling. (For CoS details, see "Class of Service" on page 355.) You can also determine where the ACE is placed in the security ACL by using the **before** *editbuffer-index* or **modify** *editbuffer-index* variables with an index number. You can use the **hits** counter to track how many packets the ACL filters.

The simplest security ACL permits or denies packets from a source IP address:

set security acl ip *acl-name* {**permit** [**cos** *cos*] | **deny**} *source-ip-addr mask* [**before** *editbuffer-index* | **modify** *editbuffer-index*]

For example, to create ACL *acl-1* that permits all packets from IP address 192.168.1.4, type the following command:

```
23x0# set security acl ip acl-1 permit 192.168.1.4 0.0.0.0
```

With the following basic security ACL command, you can specify any of the protocols supported by WSS Software:

set security acl ip *acl-name* {**permit** [**cos** *cos*] | **deny**} {*protocol*} {*source-ip-addr mask destination-ip-addr mask*} [**precedence** *precedence*] [**tos** *tos*] [**before** *editbuffer-index* | **modify** *editbuffer-index*]

The following sample security ACL permits all Generic Routing Encapsulation (GRE) packets from source IP address 192.168.1.11 to destination IP address 192.168.1.15, with a precedence level of 0 (routine), and a type-of-service (TOS) level of 0 (normal). (For more information about type-of-service and precedence levels, see the *Nortel Mobility System Software Command Reference*.) GRE is protocol number 47.

```
23x0# set security acl ip acl-2 permit cos 2 47 192.168.1.11 0.0.0.0 192.168.1.15 0.0.0.0
precedence 0 tos 0 hits
```

The security ACL *acl-2* described above also applies the CoS level 2 (medium priority) to the permitted packets. (For CoS details, see "Class of Service" on page 355.) The keyword **hits** counts the number of times this ACL affects packet traffic.

Table 22 lists common IP protocol numbers. (For a complete list of IP protocol names and numbers, see http://www.iana.org/assignments/protocol-numbers.) For commands that set security ACLs for specific protocols, see the following information:

- "Setting an ICMP ACL" on page 357
- "Setting a TCP ACL" on page 359
- "Setting a UDP ACL" on page 359

Table 22: Common IP Protocol Numbers

Number	IP Protocol
1	Internet Message Control Protocol (ICMP)
2	Internet Group Management Protocol (IGMP)
6	Transmission Control Protocol (TCP)
9	Any private interior gateway (used by Cisco for Internet Gateway Routing Protocol)

Table 22: Common IP Protocol Numbers

Number	IP Protocol
17	User Datagram Protocol (UDP)
46	Resource Reservation Protocol (RSVP)
47	Generic Routing Encapsulation (GRE) protocol
50	Encapsulation Security Payload for IPSec (IPSec-ESP)
51	Authentication Header for IPSec (IPSec-AH)
55	IP Mobility (Mobile IP)
88	Enhanced Interior Gateway Routing Protocol (EIGRP)
89	Open Shortest Path First (OSPF) protocol
103	Protocol Independent Multicast (PIM) protocol
112	Virtual Router Redundancy Protocol (VRRP)
115	Layer Two Tunneling Protocol (L2TP)

Wildcard Masks

When you specify source and destination IP addresses in an ACE, you must also include a mask for each in the form *source-ip-addr mask* and *destination-ip-addr mask.*

The mask is a wildcard mask. The security ACL checks the bits in IP addresses that correspond to any *0*s (zeros) in the mask, but does not check the bits that correspond to *1*s (ones) in the mask. Specify the IP address and wildcard mask in dotted decimal notation. For example, the IP address and wildcard mask 10.0.0.0 and 0.255.255.255 match all IP addresses that begin with 10 in the first octet.

Class of Service

Class-of-service (CoS) assignment determines the priority treatment of packets transmitted by an WSS switch, corresponding to a forwarding queue on the AP. Table 23 shows the results of CoS priorities you assign in security ACLs.

Table 23: Class-of-Service (CoS) Packet Handling

WMM Priority Desired	CLI CoS Value to Enter
Background	**1** or **2**
Best effort	**0** or **3**
Video	**4** or **5**
Voice	**6** or **7**

AP forwarding prioritization occurs automatically for Wi-Fi Multimedia (WMM) traffic. You do not need to configure ACLs to provide WMM prioritization. For non-WMM devices, you can provide AP forwarding prioritization by configuring ACLs.

If you disable WMM, AP forwarding prioritization is optimized for SpectraLink Voice Priority (SVP) instead of WMM, and the AP does not tag packets it sends to the WSS. Otherwise, the classification and tagging described in "How WMM Works in WSS Software" on page 305 remain in effect.

If you plan to use SVP or another non-WMM type of prioritization, you must configure ACLs to tag the packets. (See "Enabling Prioritization for Legacy Voice over IP" on page 376.)

Optionally, for WMM or non-WMM traffic, you can use ACLs to change the priority of traffic sent to an AP or VLAN. (To change CoS for WMM or non-WMM traffic, see "Using ACLs to Change CoS" on page 374.)

Setting an ICMP ACL

With the following command, you can use security ACLs to set Internet Control Message Protocol (ICMP) parameters for the **ping** command:

set security acl ip *acl-name* {**permit** [**cos** *cos*] | **deny**} **icmp** {*source-ip-addr mask destination-ip-addr mask*} [**type** *icmp-type*] [**code** *icmp-code*] [**precedence** *precedence*] [**tos** *tos*] [**before** *editbuffer-index* | **modify** *editbuffer-index*] [**hits**]

An ICMP ACL can filter packets by source and destination IP address, TOS level, precedence, ICMP type, and ICMP code. For example, the following command permits all ICMP packets coming from 192.168.1.3 and going to 192.168.1.4 that also meet the following conditions:

- ICMP type is 11 (Time Exceeded).
- ICMP code is 0 (Time to Live Exceeded).
- Type-of-service level is 12 (minimum delay plus maximum throughput).
- Precedence is 7 (network control).

```
23x0# set security acl ip acl-3 permit icmp 192.168.1.3 0.0.0.0 192.168.1.4 0.0.0.0 type
    11 code 0 precedence 7 tos 12 before 1 hits
```

The **before 1** portion of the ACE places it before any others in the ACL, so it has precedence over any later ACEs for any parameter settings that are met.

For more information about changing the order of ACEs or otherwise modifying security ACLs, see "Modifying a Security ACL" on page 369. For information about TOS and precedence levels, see the *Nortel Mobility System Software Command Reference*. For CoS details, see "Class of Service" on page 355.

ICMP includes many messages that are identified by a *type* field. Some also have a code within that type. Table 24 lists some common ICMP types and codes. For more information, see http://www.iana.org/assignments/icmp-parameters.

Table 24: Common ICMP Message Types and Codes

ICMP Message Type (Number)	ICMP Message Code (Number)
Echo Reply (0)	None
Destination Unreachable (3)	• Network Unreachable (0) • Host Unreachable (1) • Protocol Unreachable (2) • Port Unreachable (3) • Fragmentation Needed (4) • Source Route Failed (5)
Source Quench (4)	None
Redirect (5)	• Network Redirect (0) • Host Redirect (1) • Type of Service (TOS) and Network Redirect (2) • TOS and Host Redirect (3)

Table 24: Common ICMP Message Types and Codes (continued)

ICMP Message Type (Number)	ICMP Message Code (Number)
Echo (8)	None
Time Exceeded (11)	• Time to Live (TTL) Exceeded (0) • Fragment Reassembly Time Exceeded (1)
Parameter Problem (12)	None
Timestamp (13)	None
Timestamp Reply (14)	None
Information Request (15)	None
Information Reply (16)	None

Setting TCP and UDP ACLs

Security ACLs can filter TCP and UDP packets by source and destination IP address, precedence, and TOS level. You can apply a TCP ACL to established TCP sessions only, not to new TCP sessions. In addition, security ACLs for TCP and UDP can filter packets according to a source port on the source IP address and/or a destination port on the destination IP address, if you specify a port number and an operator in the ACE. (For a list of TCP and UDP port numbers, see http://www.iana.org/assignments/port-numbers.)

The operator indicates whether to filter packets arriving from or destined for a port whose number is equal to (**eq**), greater than (**gt**), less than (**lt**), not equal to (**neq**), or in a range that includes (**range**) the specified port. To specify a range of TCP or UDP ports, you enter the beginning and ending port numbers.



Note. The CLI does not accept port names in ACLs. To filter on ports by name, you must use WLAN Management Software . For more information, see the *Nortel WLAN Management Software Reference Manual*.

Setting a TCP ACL

The following command filters TCP packets:

set security acl ip *acl-name* {**permit** [**cos** *cos*] | **deny**} **tcp** {*source-ip-addr mask* [*operator port* [*port2*]] *destination-ip-addr mask* [*operator port* [*port2*]]} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**before** *editbuffer-index* | **modify** *editbuffer-index*] [**hits**]

For example, the following command permits packets sent from IP address 192.168.1.5 to 192.168.1.6 with the TCP destination port equal to 524, a precedence of 7, and a type of service of 15, on an established TCP session, and counts the number of hits generated by the ACE:

```
23x0# set security acl ip acl-4 permit tcp 192.168.1.5 0.0.0.0 192.168.1.6 0.0.0.0 eq 524
      precedence 7 tos 15 established hits
```

(For information about TOS and precedence levels, see the *Nortel Mobility System Software Command Reference*. For CoS details, see "Class of Service" on page 355.)

Setting a UDP ACL

The following command filters UDP packets:

set security acl ip *acl-name* {**permit** [**cos** *cos*] | **deny**} **udp** {*source-ip-addr mask* [*operator port* [*port2*]] *destination-ip-addr mask* [*operator port* [*port2*]]} [**precedence** *precedence*] [**tos** *tos*] [**before** *editbuffer-index* | **modify** *editbuffer-index*] [**hits**]

For example, the following command permits UDP packets sent from IP address 192.168.1.7 to IP address 192.168.1.8, with any UDP destination port less than 65,535. It puts this ACE first in the ACL, and counts the number of hits generated by the ACE.

```
23x0# set security acl ip acl-5 permit udp 192.168.1.7 0.0.0.0 192.168.1.8 0.0.0.0 lt 65535
      precedence 7 tos 15 before 1 hits
```

(For information about TOS and precedence levels, see the *Nortel Mobility System Software Command Reference*. For CoS details, see "Class of Service" on page 355.)

Determining the ACE Order

The **set security acl** command creates a new entry in the edit buffer and appends the new entry as a rule at the end of an ACL, unless you specify otherwise. The order of ACEs is significant, because the earliest ACE takes precedence over later ACEs. To place the ACEs in the correct order, use the parameters **before** *editbuffer-index* and **modify** *editbuffer-index*. The first ACE is number 1.

To specify the order of the commands, use the following parameters:

- **before** *editbuffer-index* inserts an ACE before a specific location.
- **modify** *editbuffer-index* changes an existing ACE.

If the security ACL you specify when creating an ACE does not exist when you enter **set security acl ip**, the specified ACL is created in the edit buffer. If the ACL exists but is not in the edit buffer, the ACL reverts, or is rolled back, to the state when its last ACE was committed, but it now includes the new ACE.

For details, see "Placing One ACE before Another" on page 371 and "Modifying an Existing Security ACL" on page 372.

Committing a Security ACL

To put the security ACLs you have created into effect, use the **commit security acl** command with the name of the ACL. For example, to commit *acl-99*, type the following command:

```
23x0# commit security acl acl-99
success: change accepted.
```

To commit all the security ACLs in the edit buffer, type the following command:

```
23x0# commit security acl all
success: change accepted.
```

Viewing Security ACL Information

To determine whether a security ACL is committed, you can check the edit buffer and the committed ACLs. After you commit an ACL, WSS Software removes it from the edit buffer.

Viewing the Edit Buffer

The edit buffer enables you to view the security ACLs you create before committing them to the configuration. To view a summary of the ACLs in the edit buffer, type the following command:

```
23x0# show security acl editbuffer
ACL edit-buffer table

ACL                              Type Status
-------------------------------- ---- -------------
acl-99                           IP   Not committed
acl-blue                         IP   Not committed
acl-violet                       IP   Not committed
```

Viewing Committed Security ACLs

To view a summary of the committed security ACLs in the configuration, type the following command:

```
23x0# show security acl
ACL table

ACL                              Type Class  Mapping
-------------------------------- ---- ------ -------
acl-2                            IP   Static
acl-3                            IP   Static
acl-4                            IP   Static
```

Viewing Security ACL Details

You can display the contents of one or all security ACLs that are committed. To display the contents of all committed security ACLs, type the following command:

```
23x0# show security acl info all
ACL information for all

set security acl ip acl-999 (hits #2 0)
---------------------------------------------------
 1. deny IP source IP 192.168.0.1 0.0.0.0 destination IP any
2. permit IP source IP 192.168.0.2 0.0.0.0 destination IP any enable-hits

set security acl ip acl-2 (hits #1 0)
---------------------------------------------------
 1. permit L4 Protocol 115 source IP 192.168.1.11 0.0.0.0 destination IP
192.168.1.15 0.0.0.0 precedence 0 tos 0 enable-hits
```

You can also view a specific security ACL. For example, to view *acl-2*, type the following command:

```
23x0# show security acl info acl-2
ACL information for acl-2

set security acl ip acl-2 (hits #1 0)
----------------------------------------------------
 1. permit L4 Protocol 115 source IP 192.168.1.11 0.0.0.0 destination IP
192.168.1.15 0.0.0.0 precedence 0 tos 0 enable-hits
```

Displaying Security ACL Hits

Once you map an ACL, you can view the number of packets it has filtered, if you included the keyword **hits**. (For information on setting hits, see "Setting a Source IP ACL" on page 354.) Type the following command:

```
23x0# show security acl hits
ACL hit-counters

Index Counter              ACL-name
----- -------------------- --------
    1                    0 acl-2
    2                    0 acl-999
    5                  916 acl-123
```

To sample the number of hits the security ACLs generate, you must specify the number of seconds between samples. For example, to sample the hits generated every 180 seconds, type the following commands:

```
23x0# hit-sample-rate 180

23x0# show security acl hits
ACL hit-counters

Index Counter              ACL-name
----- -------------------- --------
    1                31986 acl-red
    2                    0 acl-green
```

Clearing Security ACLs

The **clear security acl** command removes the ACL from the edit buffer only. To clear a security ACL, enter a specific ACL name, or enter **all** to delete all security ACLs. To remove the security ACL from the running configuration and nonvolatile storage, you must also use the **commit security acl** command.

For example, the following command deletes *acl-99* from the edit buffer:

```
23x0# clear security acl acl-99
```

To clear *acl-99* from the configuration, type the following command:

```
23x0# commit security acl acl-99
success: change accepted
```

Mapping Security ACLs

User-based security ACLs are mapped to an IEEE 802.1X authenticated session during the AAA process. You can specify that one of the authorization attributes returned during authentication is a named security ACL. The WSS switch maps the named ACL automatically to the user's authenticated session.

Security ACLs can also be mapped statically to ports, VLANs, virtual ports, or Distributed APs. User-based ACLs are processed before these ACLs, because they are more specific and closer to the network edge.

Mapping User-Based Security ACLs

When you configure administrator or user authentication, you can set a Filter-Id authorization attribute at the RADIUS server or at the WSS switch's local database. The Filter-Id attribute is a security ACL name with the direction of the packets appended—for example, *acl-name***.in** or *acl-name***.out**. The security ACL mapped by Filter-Id instructs the WSS switch to use its local definition of the ACL, including the flow direction, to filter packets for the authenticated user.



Note. The Filter-Id attribute is more often received by the WSS through an external AAA RADIUS server than applied through the local database.

To map a security ACL to a user session, follow these steps:

1. Create the security ACL. For example, to filter packets coming from 192.168.253.1 and going to 192.168.253.12, type the following command:

   23x0# **set security acl ip acl-222 permit ip 192.168.253.1 0.0.0.0 198.168.253.12 0.0.0.0 hits**

2. Commit the security ACL to the running configuration. For example, to commit *acl-222*, type the following command:

   23x0# **commit security acl acl-222**
   ```
   success: change accepted.
   ```

3. Apply the Filter-Id authentication attribute to a user's session through an external RADIUS server. For instructions, see the documentation for your RADIUS server.



Note. If the Filter-Id value returned through the authentication and authorization process does not match the name of a committed security ACL in the WSS, the user fails authorization and cannot be authenticated.

4. Alternatively, authenticate the user with the Filter-Id attribute in the WSS switch's local database. Use one of the following commands. Specify **.in** for incoming packets or **.out** for outgoing packets.

Mapping Target	Commands
User authenticated by a password	**set user** *username* **attr filter-id** *acl-name***.in** **set user** *username* **attr filter-id** *acl-name***.out**
User authenticated by a MAC address	**set mac-user** *username* **attr filter-id** *acl-name***.in** **set mac-user** *username* **attr filter-id** *acl-name***.out**

When assigned the Filter-Id attribute, an authenticated user with a current session receives packets based on the security ACL. For example, to restrict incoming packets for Natasha to those specified in *acl-222*, type the following command:

23x0# **set user Natasha attr filter-id acl-222.in**
```
success: change accepted.
```

You can also map a security ACL to a user group. For details, see “Assigning a Security ACL to a User or a Group” on page 451. For more information about authenticating and authorizing users, see “About Administrative Access” on page 54 and “AAA Tools for Network Users” on page 410.

Mapping Security ACLs to Ports, VLANs, Virtual Ports, or Distributed APs

Security ACLs can be mapped to ports, VLANs, virtual ports, and Distributed APs. Use the following command:

set security acl map *acl-name* {**vlan** *vlan-id* | **port** *port-list* [**tag** *tag-value*] | **dap** *dap-num*} {**in** | **out**}

Specify the name of the ACL, the port, VLAN, tag value(s) of the virtual port, or the number of the Distributed AP to which the ACL is to be mapped, and the direction for packet filtering. For virtual ports or Distributed APs, you can specify a single value, a comma-separated list of values, a hyphen-separated range, or any combination, with no spaces. For example, to map security ACL *acl-222* to virtual ports 1 through 3 and 5 on port 2 to filter incoming packets, type the following command:

```
23x0# set security acl map acl-222 port 2 tag 1-3,5 in
success: change accepted.
```

Plan your security ACL maps to ports, VLANs, virtual ports, and Distributed APs so that only one security ACL filters a flow of packets. If more than one security ACL filters the same traffic, you cannot guarantee the order in which the ACE rules are applied.

Displaying ACL Maps to Ports, VLANs, and Virtual Ports

Two commands display the port, VLAN, virtual port, and Distributed AP mapping of a specific security ACL. For example, to show the ports, VLANs, virtual ports, and Distributed APs mapped to *acl-999*, type one of the following commands:

```
23x0# show security acl map acl-999
ACL acl-999 is mapped to:

Port 9 In
Port 9 Out

23x0# show security acl
ACL table

ACL                              Type Class  Mapping
-------------------------------- ---- ------ -------
acl-orange                            IP   Static
acl-999                               IP   Static Port 9 In
                                                  Port 9 Out
acl-blue                              IP   Static Port 1 In
acl-violet                            IP   Static VLAN 1 Out
```

Clearing a Security ACL Map

To clear the mapping between a security ACL and one or more ports, VLANs, virtual ports, or Distributed APS, first display the mapping with **show security acl map** and then use **clear security acl map** to remove it. This command removes the mapping, but not the ACL.

For example, to clear the security ACL *acljoe* from a port, type the following commands:

```
23x0# show security acl map acljoe
ACL acljoe is mapped to:

Port 4 In

23x0# clear security acl map acljoe port 4 in
success: change accepted.
```

After you clear the mapping between port 4 and ACL *acljoe*, the following is displayed when you enter **show security acl map**:

```
23x0# show security acl map acljoe
ACL acljoe is mapped to:
```

Clearing a security ACL mapping does not stop the current filtering function if the ACL has other mappings. If the security ACL is mapped to another port, a VLAN, a virtual port, or a Distributed AP, you must enter a **clear security acl map** command to clear each map.

To stop the packet filtering of a user-based security ACL, you must modify the user's configuration in the local database on the WSS switch or on the RADIUS servers where packet filters are authorized. For information about deleting a security ACL from a user's configuration in the local WSS database, see "Clearing a Security ACL from a User or Group" on page 453. To delete a security ACL from a user's configuration on a RADIUS server, see the documentation for your RADIUS server.

If you no longer need the security ACL, delete it from the configuration with the **clear security acl** and **commit security acl** commands. (See "Clearing Security ACLs" on page 365.)

Modifying a Security ACL

You can modify a security ACL in the following ways:

- Add another ACE to a security ACL, at the end of the ACE list. (See "Adding Another ACE to a Security ACL" on page 370.)
- Place an ACE before another ACE, so it is processed before subsequent ACEs, using the **before** *editbuffer-index* portion of the **set security acl** commands. (See "Placing One ACE before Another" on page 371.)
- Modify an existing ACE using the **modify** *editbuffer-index* portion of the **set security acl** commands. (See "Modifying an Existing Security ACL" on page 372.)
- Use the **rollback** command set to clear changes made to the security ACL edit buffer since the last time it was saved. The ACL is rolled back to its state at the last **commit** command. (See "Clearing Security ACLs from the Edit Buffer" on page 373.)
- Use the **clear security acl map** command to stop the filtering action of an ACL on a port, VLAN, or virtual port. (See "Clearing a Security ACL Map" on page 368.)
- Use **clear security acl** plus **commit security acl** to completely delete the ACL from the WSS switch's configuration. (See "Clearing Security ACLs" on page 365.)

Adding Another ACE to a Security ACL

The simplest way to modify a security ACL is to add another ACE. For example, suppose you wanted to modify an existing ACL named *acl-violet.* Follow these steps:

1. To display all committed security ACLs, type the following command:

   ```
   23x0# show security acl info all
   ACL information for all

   set security acl ip acl-violet (hits #2 0)
   ---------------------------------------------------
    1. permit IP source IP 192.168.253.1 0.0.0.255 destination IP
   any enable-hits
   ```

2. To add another ACE to the end of *acl-violet*, type the following command:

   ```
   23x0# set security acl ip acl-violet permit 192.168.123.11 0.0.0.255 hits
   ```

3. To commit the updated security ACL *acl-violet*, type the following command:

   ```
   23x0# commit security acl acl-violet
   success: change accepted.
   ```

4. To display the updated *acl-violet*, type the following command:

   ```
   23x0# show security acl info all
   ACL information for all

   set security acl ip acl-violet (hits #2 0)
   ---------------------------------------------------
    1. permit IP source IP 192.168.253.1 0.0.0.255 destination IP
   any enable-hits
    2. permit IP source IP 192.168.123.11 0.0.0.255 destination IP
   any enable-hits
   ```

Placing One ACE before Another

You can use the **before** *editbuffer-index* portion of the **set security acl** command to place a new ACE before an existing ACE. For example, suppose you want to deny some traffic from IP address 192.168.254.12 in *acl-111*. Follow these steps:

1. To display all committed security ACLs, type the following command:

   23x0# **show security acl info all**

```
ACL information for all

set security acl ip acl-111 (hits #4 0)
-----------------------------------------------
 1. permit IP source IP 192.168.253.11 0.0.0.0 destination IP
any

set security acl ip acl-2 (hits #1 0)
-----------------------------------------------
 1. permit L4 Protocol 115 source IP 192.168.1.11 0.0.0.0
destination IP 192.168.1.15 0.0.0.0 precedence 0 tos 0
enable-hits
```

2. To add the deny ACE to *acl-111* and place it first, type the following commands:

   23x0# **set security acl ip acl-111 deny 192.168.254.12 0.0.0.255 before 1**

   23x0# **commit security acl acl-111**

```
success: change accepted.
```

3. To view the results, type the following command:

   23x0# **show security acl info all**

```
ACL information for all

set security acl ip acl-111 (hits #4 0)
-----------------------------------------------
 1. deny IP source IP 192.168.254.12 0.0.0.255 destination IP
any
 2. permit IP source IP 192.168.253.11 0.0.0.0 destination IP
any

set security acl ip acl-2 (hits #1 0)
-----------------------------------------------
 1. permit L4 Protocol 115 source IP 192.168.1.11 0.0.0.0
destination IP 192.168.1.15 0.0.0.0 precedence 0 tos 0
enable-hits
```

Modifying an Existing Security ACL

You can use the **modify** *editbuffer-index* portion of the **set security acl** command to modify an active security ACL. For example, suppose the ACL *acl-111* currently blocks some packets from IP address 192.168.254.12 with the mask 0.0.0.255 and you want to change the ACL to permit all packets from this address. Follow these steps:

1. To display all committed security ACLs, type the following command:

```
23x0# show security acl info all
ACL information for all

set security acl ip acl-111 (hits #4 0)
---------------------------------------------------
 1. deny IP source IP 192.168.254.12 0.0.0.255 destination IP
any
 2. permit IP source IP 192.168.253.11 0.0.0.0 destination IP
any

set security acl ip acl-2 (hits #1 0)
---------------------------------------------------
 1. permit L4 Protocol 115 source IP 192.168.1.11 0.0.0.0
destination IP 192.168.1.15 0.0.0.0 precedence 0 tos 0
enable-hits
```

2. To modify the first ACE in *acl-111*, type the following commands:

```
23x0# set security acl ip acl-111 permit 192.168.254.12 0.0.0.0 modify 1

23x0# commit security acl acl-111
success: change accepted.
```

3. To view the results, type the following command:

```
23x0# show security acl info all
ACL information for all

set security acl ip acl-111 (hits #4 0)
---------------------------------------------------
 1. permit IP source IP 192.168.254.12 0.0.0.0 destination IP
any
 2. permit IP source IP 192.168.253.11 0.0.0.0 destination IP
any

set security acl ip acl-2 (hits #1 0)
---------------------------------------------------
 1. permit L4 Protocol 115 source IP 192.168.1.11 0.0.0.0
destination IP 192.168.1.15 0.0.0.0 precedence 0 tos 0
enable-hits
```

Clearing Security ACLs from the Edit Buffer

Use the **rollback** command to clear changes made to the security ACL edit buffer since it was last committed. The ACL is rolled back to its state at the last **commit** command. For example, suppose you want to remove an ACE that you just created in the edit buffer for *acl-111*:

1. To display the contents of all committed security ACLs, type the following command:

```
23x0# show security acl info all
ACL information for all

set security acl ip acl-111 (hits #4 0)
---------------------------------------------------
 1. permit IP source IP 192.168.254.12 0.0.0.0 destination IP
any
 2. permit IP source IP 192.168.253.11 0.0.0.0 destination IP
any

set security acl ip acl-2 (hits #1 0)
---------------------------------------------------
 1. permit L4 Protocol 115 source IP 192.168.1.11 0.0.0.0
destination IP 192.168.1.15 0.0.0.0 precedence 0 tos 0
enable-hits
```

2. To view a summary of the security ACLs for which you just created ACEs in the edit buffer, type the following command:

```
23x0# show security acl editbuffer
ACL edit-buffer table

ACL                              Type Status
-------------------------------- ---- --------------
acl-a                            IP   Not committed
acl-111                          IP   Not committed
```

3. To view details about these uncommitted ACEs, type the following command. The entire *acl-111* is displayed, including its committed ACEs.

```
23x0# show security acl info all editbuffer
ACL edit-buffer information for all

set security acl ip acl-111 (ACEs 3, add 3, del 0, modified 2)
---------------------------------------------------
 1. permit IP source IP 192.168.254.12 0.0.0.0 destination IP
any
 2. permit IP source IP 192.168.253.11 0.0.0.0 destination IP
any
 3. deny SRC source IP 192.168.253.1 0.0.0.255

set security acl ip acl-a (ACEs 1, add 1, del 0, modified 0)
---------------------------------------------------
 1. permit SRC source IP 192.168.1.1 0.0.0.0
```

4. To clear the uncommitted *acl-111* ACE from the edit buffer, type the following command:

   23x0# **rollback security acl acl-111**

5. To ensure that you have cleared the *acl-111* ACE, type the following command. Only the uncommitted *acl-a* now appears.

   23x0# **show security acl info all editbuffer**

```
ACL edit-buffer information for all

set security acl ip acl-a (ACEs 1, add 1, del 0, modified 0)
-------------------------------------------------
 1. permit SRC source IP 192.168.1.1 0.0.0.0
```

6. Alternatively, to clear the entire edit buffer of all changes made since a security ACL was last committed and display the results, type the following commands:

   23x0# **rollback security acl all**

   23x0# **show security acl info all editbuffer**

```
ACL edit-buffer information for all
```

Using ACLs to Change CoS

For WMM or non-WMM traffic, you can change a packet's priority by using an ACL to change the packet's CoS value. To change CoS value using an ACL, you must map the ACL to the outbound traffic direction on an AP port, Distributed AP, or user VLAN.

For example, to remap IP packets from IP address 10.10.20.5 that have IP precedence value 3, to have CoS value 7 when they are forwarded to any 10.10.30.x address on Distributed AP 2, enter the following commands:

23x0# **set security acl ip acl1 permit cos 7 ip 10.10.20.5 0.0.0.0 10.10.30.0 0.0.0.255 precedence 3**

```
success: change accepted.
```

23x0# **set security acl ip acl1 permit 0.0.0.0 255.255.255.255**

```
success: change accepted.
```

23x0# **commit security acl acl1**

```
success: change accepted.
```

23x0# **set security acl map acl1 dap 2 out**

```
success: change accepted.
```

The default action on an interface and traffic direction that has at least one access control entry (ACE) configured, is to deny all traffic that does not match an ACE on that interface and traffic direction. The **permit 0.0.0.0 255.255.255.255** ACE ensures that traffic that does not match the first ACE is permitted. Without this additional ACE at the end, traffic that does not match the other ACE is dropped.

Filtering Based on DSCP Values

To filter based on a Differentiated Services Code Point (DSCP) value, specify the combination of precedence and ToS values that is equivalent to the DSCP value. For example, to filter based on DSCP value 46, configure an ACL that filters based on precedence 5 and ToS 12. (To display a table of the precedence and ToS combinations for each DSCP value, use the **show security acl dscp** command.)

The following commands remap IP packets from IP address 10.10.50.2 that have DSCP value 46 (equivalent to precedence value 5 and ToS value 12), to have CoS value 7 when they are forwarded to any 10.10.90.x address on Distributed AP 4:

```
23x0# set security acl ip acl2 permit cos 7 ip 10.10.50.2 0.0.0.0 10.10.90.0 0.0.0.255 precedence
    5 tos 12
success: change accepted.

23x0# set security acl ip acl2 permit cos 7 ip 10.10.50.2 0.0.0.0 10.10.90.0 0.0.0.255 precedence
    5 tos 13
success: change accepted.

23x0# set security acl ip acl2 permit 0.0.0.0 255.255.255.255
success: change accepted.

23x0# commit security acl acl2
success: change accepted.

23x0# set security acl map acl2 dap 4 out
success: change accepted.
```

The ACL contains two ACEs. The first ACE matches on precedence 5 and ToS 12. The second ACE matches on precedence 5 and ToS 13. The IP precedence and ToS fields use 7 bits, while the DSCP field uses only 6 bits. Following the DSCP field is a 2-bit ECN field that can be set by other devices based on network congestion. The second ACE is required to ensure that the ACL matches regardless of the value of the seventh bit.

Table 23 lists the CoS values to use when reassigning traffic to a different priority. The CoS determines the AP forwarding queue to use for the traffic when sending it to a wireless client.

Table 25: Class-of-Service (CoS) Packet Handling

WMM Priority Desired	CLI CoS Value to Enter
Background	**1** or **2**
Best effort	**0** or **3**
Video	**4** or **5**
Voice	**6** or **7**

Enabling Prioritization for Legacy Voice over IP

WSS Software supports Wi-Fi Multimedia (WMM). WMM support is enabled by default and is automatically used for priority traffic between WMM-capable devices.

WSS Software also can provide prioritization for non-WMM VoIP devices. However, to provide priority service to non-WMM VoIP traffic, you must configure an ACL to set the CoS for the traffic. The AP maps this CoS value to a forwarding queue.

- If you plan to leave WMM enabled, use an ACL to set the CoS for any type of non-WMM VoIP wireless traffic to 6 or 7.
- If you plan to disable WMM, set the CoS for SVP traffic to 6 or 7, but set the CoS for other types of non-WMM VoIP traffic to 4 or 5. When WMM is disabled, the AP forwarding queue that maps to CoS values 6 and 7 is optimized for SVP.



Note. If you are upgrading a switch running WSS Software Version 3.*x* to WSS Software Version 4.*x*, and the switch uses ACLs to map VoIP traffic to CoS 4 or 5, and you plan to leave WMM enabled, Nortel recommends that you change the ACLs to map the traffic to CoS 6 or 7.

You must map the ACL to the outbound traffic direction on an AP port, Distributed AP, or user VLAN. An ACL can set a packet's CoS only in these cases.

You can enable legacy VoIP support on a VLAN, port group, port list, virtual port list, Distributed AP, or user wildcard. You do not need to disable WMM support.

For example, to enable VoIP support for TeleSym packets, which use UDP port 3344, for all users in VLAN *corp_vlan*, perform the following steps:

1. Configure an ACE in ACL *voip* that assigns IP traffic from any IP address with source UDP port 3344, addressed to any destination address, to CoS queue 6:

   23x0# **set security acl ip voip permit cos 6 udp 0.0.0.0 255.255.255.255 eq 3344 0.0.0.0 255.255.255.255**

2. Configure another ACE to change the default action of the ACL from deny to permit. Otherwise, the ACL permits only voice traffic that matches the previous ACE and denies all other traffic.

   23x0# **set security acl ip voip permit 0.0.0.0 255.255.255.255**

3. Commit the ACL to the configuration:

   23x0# **commit security acl voip**

4. Map the ACL to the outbound traffic direction of VLAN *corp_vlan*:

   23x0# **set security acl map voip vlan corp_vlan out**

Enabling SVP Optimization for SpectraLink Phones

You can configure WSS Software to prioritize voice traffic for VoIP phones that use SpectraLink Voice Priority (SVP). If you disable WMM support and enable SVP support, WSS Software ensures voice quality for SpectraLink phones using SVP by allocating CoS queues 6 and 7 on the MAP for distinct SVP treatment as well as forwarding all traffic from that queue before forwarding traffic from other queues.

You can enable SVP optimization on a VLAN, port group, port list, virtual port list, Distributed AP, or user wildcard. To enable SVP optimization, disable WMM support on the radio profile that serves the SVP users, configure an ACL that assigns traffic for IP protocol 119 to CoS queue 6 or 7, and map the ACL to the outbound traffic direction.

For example, to enable SVP support for all users in VLAN *corp_vlan*, perform the following steps:

1. Disable WMM support on the radio profile that will serve SVP users, to enable SVP optimization on AP forwarding queues 6 and 7 for radios managed by that radio profile:

   23x0# **set radio-profile radprofsvp wmm disable**

2. Configure an ACE in ACL *svp* that assigns IP protocol 119 traffic for all source and destination addresses to CoS queue 7:

   23x0# **set security acl ip svp permit cos 7 119 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255**

3. Configure another ACE to change the default action of the ACL from deny to permit. Otherwise, the ACL permits only voice traffic that matches the previous ACE and denies all other traffic.

   23x0# **set security acl ip svp permit 0.0.0.0 255.255.255.255**

4. Commit the ACL to the configuration:

   23x0# **commit security acl svp**

5. Map the ACL to the outbound traffic direction of VLAN *corp_vlan*:

   23x0# **set security acl map voip vlan corp_vlan out**

Security ACL Configuration Scenario

The following scenario illustrates how to create a security ACL named *acl-99* that consists of one ACE to permit incoming packets from one IP address, and how to map the ACL to a port and a user:

1. Type the following command to create and name a security ACL and add an ACE to it.

   23x0# **set security acl ip acl-99 permit 192.168.1.1 0.0.0.0**

2. To view the ACE you have entered, type the following command:

   23x0# **show security acl editbuffer**

```
ACL                                 Type Status
----------------------------------- ---- -------------
acl-99                              IP   Not committed
```

3. To save *acl-99* and its associated ACE to the configuration, type the following command:

   23x0# **commit security acl acl-99**

```
success: change accepted.
```

4 To map *acl-99* to port 9 to filter incoming packets, type the following command:

```
23x0# set security acl map acl-99 port 9 in
mapping configuration accepted
```

Because every security ACL includes an implicit rule denying all traffic that is not permitted, port 9 now accepts packets only from 192.168.1.1, and denies all other packets.

5 To map *acl-99* to user Natasha's sessions when you are using the local WSS database for authentication, configure Natasha in the database with the Filter-Id attribute. Type the following commands:

```
23x0# set authentication dot1x Natasha local
success: change accepted.
```

```
23x0# set user natasha attr filter-id acl-99.in
success: change accepted.
```

6 Alternatively, you can map *acl-99* to Natasha's sessions when you are using a remote RADIUS server for authentication. To configure Natasha for pass-through authentication to the RADIUS server *shorebirds*, type the following command:

```
23x0# set authentication dot1x Natasha pass-through shorebirds
success: change accepted.
```

You must then map the security ACL to Natasha's session in RADIUS. For instructions, see the documentation for your RADIUS server.

7 To save your configuration, type the following command:

```
23x0# save config
success: configuration saved.
```

Managing Keys and Certificates

Why Use Keys and Certificates? 379
About Keys and Certificates 381
Creating Keys and Certificates 385
Displaying Certificate and Key Information 393
Key and Certificate Configuration Scenarios 393

A digital certificate is a form of electronic identification for computers. The WSS switch requires digital certificates to authenticate its communications to WLAN Management Software and Web View, to Web-based AAA clients, and to Extensible Authentication Protocol (EAP) clients for which the WSS performs all EAP processing. Certificates can be generated on the WSS or obtained from a certificate authority (CA). Keys contained within the certificates allow the WSS, its servers, and its wireless clients to exchange information secured by encryption.



Note. Before installing a certificate, verify with the **show timedate** and **show timezone** commands that the WSS switch is set to the correct date, time, and time zone. Otherwise, certificates might not be installed correctly.

Why Use Keys and Certificates?

Certain WSS switch operations require the use of public-private key pairs and digital certificates. All WLAN Management Software and Web View users, and users for which the WSS performs IEEE 802.1X EAP authentication or Web-based AAA, require public-private key pairs and digital certificates to be installed on the WSS switch.

These keys and certificates are fundamental to securing wireless, wired authentication, and administrative connections because they support Wi-Fi Protected Access (WPA) encryption and dynamic Wired-Equivalency Privacy (WEP) encryption.

Wireless Security through TLS

In the case of wireless or wired authentication 802.1X users whose authentication is performed by the WSS switch, the first stage of any EAP transaction is Transport Layer Security (TLS) authentication and encryption. WLAN Management Software and Web View also require a session to the WSS that is authenticated and encrypted by TLS. Once a TLS session is authenticated, it is encrypted.

TLS allows the client to authenticate the WSS (and optionally allows the WSS to authenticate the client) through the use of digital signatures. Digital signatures require a public-private key pair. The signature is created with a private key and verified with a public key. TLS enables secure key exchange.

PEAP-MS-CHAP-V2 Security

PEAP performs a TLS exchange for server authentication and allows a secondary authentication to be performed inside the resulting secure channel for client authentication. For example, the Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP-V2) performs mutual MS-CHAP-V2 authentication inside an encrypted TLS channel established by PEAP.

1. To form the encrypted TLS channel, the WSS must have a digital certificate and must send that certificate to the wireless client.
2. Inside the WSS switch's digital certificate is the WSS's public key, which the wireless client uses to encrypt a pre-master secret key.
3. The wireless client then sends the key back to the WSS so that both the WSS and the client can derive a key from this pre-master secret for secure authentication and wireless session encryption.

Clients authenticated by PEAP need a certificate in the WSS only when the switch performs PEAP locally, not when EAP processing takes place on a RADIUS server. (For details about authentication options, see Chapter , "Configuring AAA for Network Users," on page 401.)

About Keys and Certificates

Public-private key pairs and digital signatures and certificates allow keys to be generated dynamically so that data can be securely encrypted and delivered. You generate the key pairs and certificates on the WSS or install them on the switch after enrolling with a certificate authority (CA). The WSS can generate key pairs, self-signed certificates, and Certificate Signing Requests (CSRs), and can install key pairs, server certificates, and certificates generated by a CA.



Note. The WSS uses separate *server* certificates for Admin, EAP (802.1X), and Web AAA authentication. Where applicable, the manuals refer to these server certificates as Admin, EAP (or 802.1X), or Web AAA certificates respectively.

When the WSS needs to communicate with WLAN Management Software , Web View, or an 802.1X or Web-based AAA client, WSS Software requests a private key from the switch's certificate and key store:

- If no private key is available in the WSS's certificate and key store, the switch does not respond to the request from WSS Software. If the switch does have a private key in its key store, WSS Software requests a corresponding certificate.
- If the WSS has a self-signed certificate in its certificate and key store, the switch responds to the request from WSS Software. If the certificate is not self-signed, the switch looks for a CA's certificate with which to validate the server certificate.
- If the WSS has no corresponding CA certificate, the switch does not respond to the request from WSS Software. If the switch does have a corresponding CA certificate, and the server certificate is validated (date still valid, signature approved), the switch responds.

If the WSS switch does not respond to the request from WSS Software, authentication fails and access is denied.

For EAP (802.1X) users, the public-private key pairs and digital certificates can be stored on a RADIUS server. In this case, the WSS switch operates as a pass-through authenticator.

Public Key Infrastructures

A public-key infrastructure (PKI) is a system of digital certificates and certification authorities that verify and authenticate the validity of each party involved in a transaction through the use of public key cryptography. To have a PKI, the WSS switch requires the following:

- A public key
- A private key
- Digital certificates
- A CA
- A secure place to store the private key

A PKI enables you to securely exchange and validate digital certificates between WSSs, servers, and users so that each device can authenticate itself to the others.

Public and Private Keys

Nortel's identity-based networking uses public key cryptography to enforce the privacy of data transmitted over the network. Using public-private key pairs, users and devices can send encrypted messages that only the intended receiver can decrypt.

Before exchanging messages, each party in a transaction creates a key pair that includes the public and private keys. The public key encrypts data and verifies digital signatures, and the corresponding private key decrypts data and generates digital signatures. Public keys are freely exchanged as part of digital certificates. Private keys are stored securely.

Digital Certificates

Digital certificates bind the identity of network users and devices to a public key. Network users must authenticate their identity to those with whom they communicate, and must be able to verify the identity of other users and network devices, such as switches and RADIUS servers.

The Nortel Mobility System supports the following types of X.509 digital certificates:

- **Administrative certificate**—Used by the WSS to authenticate itself to WLAN Management Software or Web View.
- **EAP certificate**—Used by the WSS to authenticate itself to EAP clients.
- **Web-based AAA certificate**—Used by the WSS to authenticate itself to Web-based AAA clients, who use a web page served by an WSS switch to log onto the network.
- **Certificate authority (CA) certificates**—Used by the WSS in addition to the certificates listed above, when those certificates are from the CA.

The Admin, EAP, and Web-based AAA certificates can be generated by the WSS (self-signed) or generated and signed by a CA. If they are signed by a CA, the CA's own certificate is also required.

PKCS #7, PKCS #10, and PKCS #12 Object Files

Public-Key Cryptography Standards (PKCS) are encryption interface standards created by RSA Data Security, Inc., that provide a file format for transferring data and cryptographic information. Nortel supports the PKCS object files listed in Table 26.

Table 26: PKCS Object Files Supported by Nortel

File Type	Standard	Purpose
PKCS #7	Cryptographic Message Syntax Standard	Contains a digital certificate signed by a CA. To install the certificate from a PKCS #7 file, use the **crypto certificate** command to prepare WSS Software to receive the certificate, then copy and paste the certificate into the CLI. A PKCS #7 file does not contain the public key to go with the certificate. Before you generate the CSR and instal the certificate, you must generate the public-private key pair using the **crypto generate key** command.
PKCS #10	Certification Request Syntax Standard	Contains a Certificate Signing Request (CSR), a special file with encoded information needed to request a digital certificate from a CA. To generate the request, use the **crypto generate request** command. Copy and paste the results directly into a browser window on the CA server, or into a file to send to the CA server.
PKCS #12	Personal Information Exchange Syntax Standard	Contains a certificate signed by a CA *and* a public-private key pair provided by the CA to go with the certificate. Because the key pair comes from the CA, you do not need to generate a key pair or a certificate request on the switch. Instead, use the **copy tftp** command to copy the file onto the WSS switch. Use the **crypto otp** command to enter the one-time password assigned to the file by the CA. (This password secures the file so that the keys and certificate cannot be installed by an unauthorized party. You must know the password in order to install them.) Use the **crypto pkcs12** command to unpack the file.

Creating Keys and Certificates

You must create a public-private key pair, and request, accept, or generate a digital certificate to exchange with WLAN Management Software or Web View for management access, or with 802.1X or Web-based AAA users for network access. The digital certificates can be self-signed or signed by a certificate authority (CA). If you use certificates signed by a CA, you must also install a certificate from the CA to validate the digital signatures of the certificates installed on the WSS.

Each of the following types of access requires a separate key pair and certificate:

- Admin—Administrative access through WLAN Management Software or Web View
- EAP—802.1X access for network users who can access SSIDs encrypted by WEP or WPA, and for users connected to wired authentication ports

- Web-based AAA—Web access for network users who can use a web page to log onto an unencrypted SSID

Management access to the CLI through Secure Shell (SSH) also requires a key pair, but does not use a certificate. (For more SSH information, see "Managing SSH" on page 123.)

Choosing the Appropriate Certificate Installation Method for Your Network

Depending on your network environment, you can use any of the following methods to install certificates and their public-private key pairs. The methods differ in terms of simplicity and security. The simplest method is also the least secure, while the most secure method is slightly more complex to use.

- **Self-signed certificate**—The easiest method to use because a CA server is not required. The WSS switch generates and signs the certificate itself. This method is the simplest but is also the least secure, because the certificate is not validated (signed) by a CA.
- **PKCS #12 object file certificate**—More secure than using self-signed certificates, but slightly less secure than using a Certificate Signing Request (CSR), because the private key is distributed in a file from the CA instead of generated by the WSS switch itself. The PKCS #12 object file is more complex to deal with than self-signed certificates. However, you can use WLAN Management Software , Web View, or the CLI to distribute this certificate. The other two methods can be performed only using the CLI.
- **Certificate Signing Request (CSR)**—The most secure method, because the WSS switch's public and private keys are created on the WSS switch itself, while the certificate comes from a trusted source (CA). This method requires generating the key pair, creating a CSR and sending it to the CA, cutting and pasting the certificate signed by the CA into the CLI, and then cutting and pasting the CA's own certificate into the CLI.

Table 27 lists the steps required for each method and refers you to appropriate instructions. (For complete examples, see "Key and Certificate Configuration Scenarios" on page 393.)

Table 27: Procedures for Creating and Validating Certificates

Certificate Installation Method	Steps Required	Instructions
Self-signed certificate	1. Generate a public-private key pair on the WSS switch. 2. Generate a self-signed certificate on the WSS switch.	• "Creating Public-Private Key Pairs" on page 388 • "Generating Self-Signed Certificates" on page 389
PKCS #12 object file certificate	1. Copy a PKCS #12 object file (public-private key pair, server certificate, and CA certificate) from a CA onto the WSS switch. 2. Enter the one-time password to unlock the file. 3. Unpack the file into the switch's certificate and key store.	"Installing a Key Pair and Certificate from a PKCS #12 Object File" on page 390
Certificate Signing Request (CSR) certificate	1. Generate a public-private key pair on the WSS switch. 2. Generate a CSR on the switch as a PKCS #10 object file. 3. Give the CSR to a CA and receive a signed certificate (a PEM-encoded PKCS #7 object file). 4. Paste the PEM-encoded file into the CLI to store the certificate on the WSS switch. 5. Obtain and install the CA's own certificate.	• "Creating Public-Private Key Pairs" on page 388 • "Creating a CSR and Installing a Certificate from a PKCS #7 Object File" on page 391 • "Installing a CA's Own Certificate" on page 392

Creating Public-Private Key Pairs

To use a self-signed certificate or Certificate Signing Request (CSR) certificate for WSS switch authentication, you must generate a public-private key pair.

To create a public-private key pair, use the following command:

crypto generate key {admin | eap | ssh | webaaa} {512 | 1024 | 2048}

Choose the key length based on your need for security or to conform with your organization's practices. For example, the following command generates an administrative key pair of 1024 bits:

```
23x0# crypto generate key admin 1024
admin key pair generated
```



Note. After you generate or install a certificate (described in the following sections), do not create the key pair again. If you do, the certificate might not work with the new key, in which case you will need to regenerate or reinstall the certificate.

Generating Self-Signed Certificates

After creating a public-private key pair, you can generate a self-signed certificate. To generate a self-signed certificate, use the following command:

crypto generate self-signed {admin | eap | webaaa}

When you type the command, the CLI Prompts you to enter information to identify the certificate. For example:

```
23x0# crypto generate self-signed admin
Country Name: US
State Name: CA
Locality Name: San Jose campus
Organizational Name: nortel
Organizational Unit: eng
Common Name: WSS1
Email Address: admin@example.com
Unstructured Name: WSS in wiring closet 120
```

You *must* include a common name (string) when you generate a self-signed certificate. The other information is optional. Use a fully qualified name if such names are supported on your network. The certificate appears after you enter this information.

Installing a Key Pair and Certificate from a PKCS #12 Object File

PKCS object files provide a file format for storing and transferring storing data and cryptographic information. (For more information, see "PKCS #7, PKCS #10, and PKCS #12 Object Files" on page 385.) A PKCS #12 object file, which you obtain from a CA, includes the private key, a certificate, and optionally the CA's own certificate.

After transferring the PKCS #12 file from the CA through FTP and generating a one-time password to unlock it, you store the file in the WSS switch's certificate and key store. To set and store a PKCS #12 object file, follow these steps:

1. Copy the PKCS #12 object file to nonvolatile storage on the WSS. Use the following command:

   copy tftp://*filename local-filename*

2. Enter a one-time password (OTP) to unlock the PKCS #12 object file. The password must be the same as the password protecting the PKCS #12 file.

   The password must contain at least 1 alphanumeric character, with no spaces, and must not include the following characters:

   - Quotation marks (“”)
   - Question mark (?)
   - Ampersand (&)

   Note. On an WSS that handles communications to or from Microsoft Windows clients, use a one-time password of 31 characters or fewer.

   To enter the one-time password, use the following command:

   crypto otp {**admin** | **eap** | **webaaa**} *one-time-password*

3. Unpack the PKCS #12 object file into the certificate and key storage area on the WSS switch. Use the following command:

   crypto pkcs12 {**admin** | **eap** | **webaaa**} *filename*

   The *filename* is the location of the file on the WSS switch.

   Note. WSS Software erases the OTP password entered with the **crypto otp** command when you enter the **crypto pkcs12** command.

Creating a CSR and Installing a Certificate from a PKCS #7 Object File

After creating a public-private key pair, you can obtain a signed certificate of authenticity from a CA by generating a Certificate Signing Request (CSR) from the WSS switch. A CSR is a text block with an encoded request for a signed certificate from the CA.

Note. Many certificate authorities have their own unique requirements. Follow the instructions in the documentation for your CA to properly format the fields you complete when generating a CSR.

1 To generate a request for a CA-signed certificate, use the following command:

crypto generate request {**admin** | **eap** | **webaaa**}

When prompted, enter values for each of six identification fields.

You must include a common name (string) when you generate a CSR. Use a fully qualified name if such names are supported on your network. The other information is optional. For example:

```
23x0# crypto generate request admin
Country Name: US
State Name: MI
Locality Name: Detroit
Organizational Name: example
Organizational Unit: eng
Common Name: WSS-34
Email Address: admin@example.com
Unstructured Name: south tower, wiring closet 125
```

When completed successfully, the command returns a Privacy-Enhanced Mail (PEM)-formatted PKCS #10 CSR. PEM encoding is a way of representing a non-ASCII file format in ASCII characters. The encoded object is the PKCS #10 CSR. Give the CSR to a CA and receive a signed certificate (a PEM-encoded PKCS #7 object file).

2 To install a certificate from a PKCS #7 file, use the following command to prepare the switch to receive it:

crypto certificate {**admin** | **eap** | **webaaa**} *PEM-formatted certificate*

3 Use a text editor to open the PKCS #7 file, and copy and paste the entire text block, including the beginning and ending delimiters, into the CLI.

Note. You must paste the entire block, from the beginning -----BEGIN CERTIFICATE REQUEST----- to the end -----END CERTIFICATE REQUEST-----.

Installing a CA's Own Certificate

If you installed a CA-signed certificate from a PKCS #7 file, you must also install the PKCS #7 certificate of that CA. (If you used the PKCS #12 method, the CA's certificate is usually included with the key pair and server certificate.)

To install a CA's certificate, use the following command:

crypto ca-certificate {admin | eap | webaaa} *PEM-formatted-certificate*

When prompted, paste the certificate under the prompt. For example:

```
23x0# crypto ca-certificate admin
Enter PEM-encoded certificate
-----BEGIN CERTIFICATE-----
MIIDwDCCA2qgAwIBAgIQL2jvuu4PO5FAQCyewU3ojANBgkqhkiG9w0BAQUFADCB
mzerMClaweVQQTTooewi\wpoer0QWNFNkj90044mbdrl1277SWQ8G7DiwYUtrqoQplKJ
.....
Lm8wmVYxP56M;CUAm908C2foYgOY40=
-----END CERTIFICATE-----
```

Displaying Certificate and Key Information

To display information about certificates installed on an WSS switch, use the following commands:

show crypto ca-certificate {admin | eap | webaaa}

show crypto certificate {admin | eap | webaaa}

For example, to display information about an administrative certificate, type the following command:

```
23x0# show crypto certificate admin
Certificate:
  Version: 3
  Serial Number:  999 (0x3e7)
  Subject: C=US, ST=CA, L=PLEAS, O=NORTEL, OU=SQA, CN=BOBADMIN/
emailAddress=BOBADMIN, unstructuredName=BOB
  Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, ST=CA, L=PLEAS, O=NORTEL, OU=SQA, CN=BOBADMIN/
emailAddress=BOBADMIN, unstructuredName=BOB
  Validity:
      Not Before: Oct 19 01:57:13 2004 GMT
      Not After : Oct 19 01:57:13 2005 GMT
```

The last two rows of the display indicate the period for which the certificate is valid. Make sure the date and time set on the switch are within the date and time range of the certificate.

Key and Certificate Configuration Scenarios

The first scenario shows how to generate self-signed certificates. The second scenario shows how to install CA-signed certificates using PKCS #12 object files, and the third scenario shows how to install CA-signed certificates using CSRs (PKCS #10 object files) and PKCS #7 object files.

(For SSH configuration information, see "Managing SSH" on page 123.)

Creating Self-Signed Certificates

To manage the security of the WSS switch for administrative access by WLAN Management Software and Web View, and the security of communication with 802.1X users and Web AAA users, create Admin, EAP, and Web AAA public-private key pairs and self-signed certificates. Follow these steps:

1. Set time and date parameters, if not already set. (See "Configuring and Managing Time Parameters" on page 136.)
2. Generate public-private key pairs:

```
23x0# crypto generate key admin 1024
key pair generated

23x0# crypto generate key eap 1024
key pair generated

23x0# crypto generate key webaaa 1024
key pair generated
```

3. Generate self-signed certificates:

```
23x0# crypto generate self-signed admin
Country Name: US
State Name: CA
Locality Name: San Francisco
Organizational Name: example
Organizational Unit: IT
Common Name: WSS 6
Email Address: admin@example.com
Unstructured Name: WSS in wiring closet 4
Self-signed cert for admin is
-----BEGIN CERTIFICATE-----
MIICUzCCAbygAwIBAgICA+cwDQYJKoZIhvcNAQEEBQAwNjELMAkGA1UEBhMCVVW
SS
CzAJBgNVBAgTAkNBMRowGAYDVQQDFBF0ZWNocHVic0B0cnB6LmNvbTAeFw0wMzA
0
...
Lm8wmVYLxP56APCUAm9O8C2foYgOY40=

-----END CERTIFICATE-----23x0# crypto generate self-signed eap
Country Name: US
State Name: CA
Locality Name: San Francisco
Organizational Name: example
Organizational Unit: IT
Common Name: WSS 6
Email Address: admin@example.com
Unstructured Name: WSS in wiring closet 4
Self-signed cert for eap is
-----BEGIN CERTIFICATE-----
```

```
MIICUzCCAbygAwIBAgICA+cwDQYJKoZIhvcNAQEEBQAwNjELMAkGA1UEBhMCVVW
SS
CzAJBgNVBAgTAkNBMRowGAYDVQQDFBF0ZWNocHVic0B0cnB6LmNvbTAeFw0wMzA
0
...
Lm8wmVYLxP56MWSS-
```

```
20# crypto generate self-signed webaaa
Country Name: US
State Name: CA
Locality Name: San Francisco
Organizational Name: example
Organizational Unit: IT
Common Name: WSS 6
Email Address: admin@example.com
Unstructured Name: WSS in wiring closet 4
Self-signed cert for webaaa is
-----BEGIN CERTIFICATE-----
MIICUzCCAbygAwIBAgICA+cwDQYJKoZIhvcNAQEEBQAwNjELMAkGA1UEBhMCVVW
SS
CzAJBgNVBAgTAkNBMRowGAYDVQQDFBF0ZWNocHVic0B0cnB6LmNvbTAeFw0wMzA
0
...
Lm8wmVYLxP56M
```

4 Display certificate information for verification:

```
23x0# show crypto certificate admin
Certificate:
  Version: 3
  Serial Number:  999 (0x3e7)
  Subject: C=US, ST=CA, L=PLEAS, O=NORTEL, OU=SQA, CN=BOBADMIN/
emailAddress=BOBADMIN, unstructuredName=BOB
  Signature Algorithm: md5WithRSAEncryption
  Issuer: C=US, ST=CA, L=PLEAS, O=NORTEL, OU=SQA, CN=BOBADMIN/
emailAddress=BOBADMIN, unstructuredName=BOB
  Validity:
      Not Before: Oct 19 01:57:13 2004 GMT
      Not After : Oct 19 01:57:13 2005 GMT
```

```
23x0# show crypto certificate eap
Certificate:
  Version: 3
  Serial Number:  999 (0x3e7)
  Subject: C=US, ST=CA, L=PLEAS, O=NORTEL, OU=SQA, CN=BOBADMIN/
emailAddress=BOBADMIN, unstructuredName=BOB
  Signature Algorithm: md5WithRSAEncryption
  Issuer: C=US, ST=CA, L=PLEAS, O=NORTEL, OU=SQA, CN=BOBADMIN/
emailAddress=BOBADMIN, unstructuredName=BOB
```

```
  Validity:
      Not Before: Oct 19 01:59:42 2004 GMT
      Not After : Oct 19 01:59:42 2005 GMT
```

23x0# **show crypto certificate webaaa**

```
Certificate:
  Version: 3
  Serial Number:  999 (0x3e7)
  Subject: C=US, ST=CA, L=PLEAS, O=NORTEL, OU=SQA, CN=BOBADMIN/
emailAddress=BOBADMIN, unstructuredName=BOB
  Signature Algorithm: md5WithRSAEncryption
  Issuer: C=US, ST=CA, L=PLEAS, O=NORTEL, OU=SQA, CN=BOBADMIN/
emailAddress=BOBADMIN, unstructuredName=BOB
  Validity:
      Not Before: Oct 19 02:02:02 2004 GMT
      Not After : Oct 19 02:02:02 2005 GMT
```

Installing CA-Signed Certificates from PKCS #12 Object Files

This scenario shows how to use PKCS #12 object files to install public-private key pairs, CA-signed certificates, and CA certifies for administrative access, 802.1X (EAP) access, and Web AAA access.

1. Set time and date parameters, if not already set. (See "Configuring and Managing Time Parameters" on page 136.)
2. Obtain PKCS #12 object files from a certificate authority.
3. Copy the PKCS #12 object files to nonvolatile storage on the WSS. Use the following command:

   copy tftp://*filename local-filename*

   For example, to copy PKCS #12 files named 2048admn.p12, 20481x.p12, and 2048web.p12 from the TFTP server at the address 192.168.253.1, type the following commands:

   23x0# **copy tftp://192.168.253.1/2048admn.p12 2048admn.p12**
   ```
   success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
   ```

   23x0# **copy tftp://192.168.253.1/20481x.p12 20481x.p12**
   ```
   success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
   ```

   23x0# **copy tftp://192.168.253.1/2048web.p12 2048web.p12**
   ```
   success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
   ```
4. Enter the one-time passwords (OTPs) for the PKCS #12 object files. The OTP protects the PKCS #12 file.

   To enter a one-time password, use the following command:

   crypto otp {**admin** | **eap** | **webaaa**} *one-time-password*

   For example:

   23x0# **crypto otp admin SeC%#6@o%c**
   ```
   OTP set
   ```

   23x0# **crypto otp eap SeC%#6@o%d**
   ```
   OTP set
   ```

   23x0# **crypto otp web SeC%#6@o%e**
   ```
   OTP set
   ```
5. Unpack the PKCS #12 object files into the certificate and key storage area on the WSS switch. Use the following command:

   crypto pkcs12 {**admin** | **eap** | **webaaa**} *filename*

   The *filename* is the location of the file on the WSS switch.

   For example:

   23x0# **crypto pkcs12 admin 2048admn.p12**
   ```
   Unwrapped from PKCS12 file:
           keypair
           device certificate
           CA certificate
   ```

```
23x0# crypto pkcs12 eap 20481x.p12
Unwrapped from PKCS12 file:
        keypair
        device certificate
        CA certificate
23x0# crypto pkcs12 web 2048web.p12
Unwrapped from PKCS12 file:
        keypair
        device certificate
        CA certificate
```



Note. WSS Software erases the OTP password entered with the **crypto otp** command when you enter the **crypto pkcs12** command.

Installing CA-Signed Certificates Using a PKCS #10 Object File (CSR) and a PKCS #7 Object File

This scenario shows how to use CSRs to install public-private key pairs, CA-signed certificates, and CA certifies for administrative access, 802.1X (EAP) access, and Web AAA access.

1. Set time and date parameters, if not already set. (See "Configuring and Managing Time Parameters" on page 136.)
2. Generate public-private key pairs:

```
23x0# crypto generate key admin 1024
key pair generated

23x0# crypto generate key eap 1024
key pair generated

23x0# crypto generate key webaaa 1024
key pair generated
```

3. Create a CSR (PKCS #10 object file) to request an administrative certificate:

```
23x0# crypto generate request admin
Country Name: US
State Name: CA
Locality Name: Cambria
Organizational Name: example
Organizational Unit: eng
Common Name: WSS-2350
Email Address: admin@example.com
Unstructured Name: wiring closet 12
CSR for admin is
-----BEGIN CERTIFICATE REQUEST-----
MIIBdTCB3wIBADA2MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExGjAYBgNVBAM
U
EXRlY2hwdWJzQHRycHouY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC
4
...
2L8Q9tk+G2As84QYMwe9RJAjfbYM5bdWRUFiLzvK7BJgqBsCZz4DP00=
-----END CERTIFICATE REQUEST-----
```

4. Copy the CSR into the CA's application.

> **Note.** You must paste the entire block, from the beginning -----BEGIN CERTIFICATE REQUEST----- to the end -----END CERTIFICATE REQUEST-----.

5. Transfer the signed administrative certificate (PKCS #7 object file) from the CA to your computer.
6. Open the signed certificate file with a text editor. Copy the entire file from the first hyphen to the last.

7. To install the administrative certificate on the WSS switch, type the following command to display a prompt:

   23x0# **crypto certificate admin**
   Enter PEM-encoded certificate

8. Paste the signed certificate text block into the WSS switch's CLI, below the prompt.
9. Display information about the certificate, to verify it:

   23x0# **show crypto certificate admin**

10. Repeat step 3 through step 9 to obtain and install EAP (802.1X) and Web AAA certificates.
11. Obtain the CA's own certificate.
12. To install the CA's certificate on the WSS switch and help authenticate the switch's Admin certificate, type the following command to display a prompt:

    23x0# **crypto ca-certificate admin**
    Enter PEM-encoded certificate

13. Paste the CA's signed certificate under the prompt.
14. Display information about the CA's certificate, to verify it:

    23x0# **show crypto ca-certificate admin**

15. Repeat step 12 through step 14 to install the CA's certificate for EAP (802.1X) and Web AAA.

Configuring AAA for Network Users

About AAA for Network Users 401
AAA Tools for Network Users 410
Configuring 802.1X Authentication 417
Configuring Authentication and Authorization by MAC Address 425
Configuring Web-based AAA 428
Configuring Last-Resort Access 440
Configuring AAA for Users of Third-Party APs 441
Assigning Authorization Attributes 446
Overriding or Adding Attributes Locally with a Location Policy 455
Configuring Accounting for Wireless Network Users 460
Displaying the AAA Configuration 464
Avoiding AAA Problems in Configuration Order 465
Configuring a Mobility Profile 468
Network User Configuration Scenarios 469

About AAA for Network Users

Network users include the following types of users:

- Wireless users—Users who access the network by associating with an SSID on a Nortel radio.
- Wired authentication users—Users who access the network over an Ethernet connection to an WSS switch port that is configured as a wired authentication (*wired-auth*) port.

You can configure authentication rules for each type of user, on an individual SSID or wired authentication port basis. WSS Software authenticates users based on user information on RADIUS servers or in the WSS switch's local database. The RADIUS servers or local database authorize successfully authenticated users for specific network access, including VLAN membership. Optionally, you also can configure accounting rules to track network access information.

The following sections describe the WSS Software authentication, authorization, and accounting (AAA) features in more detail.

Authentication

When a user attempts to access the network, WSS Software checks for an authentication rule that matches the following parameters:

- For wireless access, the authentication rule must match the SSID the user is requesting, and the user's username or MAC address.
- For access on a wired authentication port, the authentication rule must match the user's username or MAC address.

If a matching rule is found, WSS Software then checks RADIUS servers or the switch's local user database for credentials that match those presented by the user. Depending on the type of authentication rule that matches the SSID or wired authentication port, the required credentials are the username or MAC address, and in some cases, a password.

Each authentication rule specifies where the user credentials are stored. The location can be a group of RADIUS servers or the switch's local database. In either case, if WSS Software has an authentication rule that matches on the required parameters, WSS Software checks the username or MAC address of the user and, if required, the password to make sure they match the information configured on the RADIUS servers or in the local database.

The username or MAC address can be an exact match or can match a userwildcard or MAC address wildcard, which allow wildcards to be used for all or part of the username or MAC address. (For more information about wildcards, see "AAA Tools for Network Users" on page 410.)

Authentication Types

WSS Software provides the following types of authentication:

- IEEE 802.1X—If the network user's network interface card (NIC) supports 802.1X, WSS Software checks for an 802.1X authentication rule that matches the username (and SSID, if wireless access is requested), and that uses the Extensible Authentication Protocol (EAP) requested by the NIC. If a matching rule is found, WSS Software uses the requested EAP to check the RADIUS server group or local database for the username and password entered by the user. If matching information is found, WSS Software grants access to the user.
- MAC—If the username does not match an 802.1X authentication rule, but the MAC address of the user's NIC or Voice-over-IP (VoIP) phone and the SSID (if wireless) do match a MAC authentication rule, WSS Software checks the RADIUS server group or local database for matching user information. If the MAC address (and password, if on a RADIUS server) matches, WSS Software grants access. Otherwise, WSS Software attempts the fallthru authentication type, which can be Web, last-resort, or none. (Fallthru authentication is described in more detail in "Authentication Algorithm" on page 403.)
- Web—A network user attempts to access a web page over the network. The WSS switch intercepts the HTTP or HTTPS request and serves a login Web page to the user. The user enters the username and password, and WSS Software checks the RADIUS server group or local database for matching user information. If the username and password match, WSS Software redirects the user to the web page she requested. Otherwise, WSS Software denies access to the user.
- Last-resort—A network user requests access to the network, without entering a username or password. WSS Software checks for a last-resort authentication rule for the requested SSID (or for **wired**, if the user is on a wired authentication port). If a matching rule is found, WSS Software checks the RADIUS server group or local database for username **last-resort-wired** (for wired authentication access) or **last-resort-*ssid***, where ***ssid*** is the SSID requested by the user. If the user information is on a RADIUS server, WSS Software also checks for a password.

Authentication Algorithm

WSS Software can try more than one of the authentication types described in "Authentication Types" to authenticate a user. WSS Software tries 802.1X first. If the user's NIC supports 802.1X but fails authentication, WSS Software denies access. Otherwise, WSS Software tries MAC authentication next. If MAC authentication is successful, WSS Software grants access to the user. Otherwise, WSS Software tries the *fallthru* authentication type specified for the SSID or wired authentication port. The fallthru authentication type can be one of the following:

- Web
- Last-resort
- None

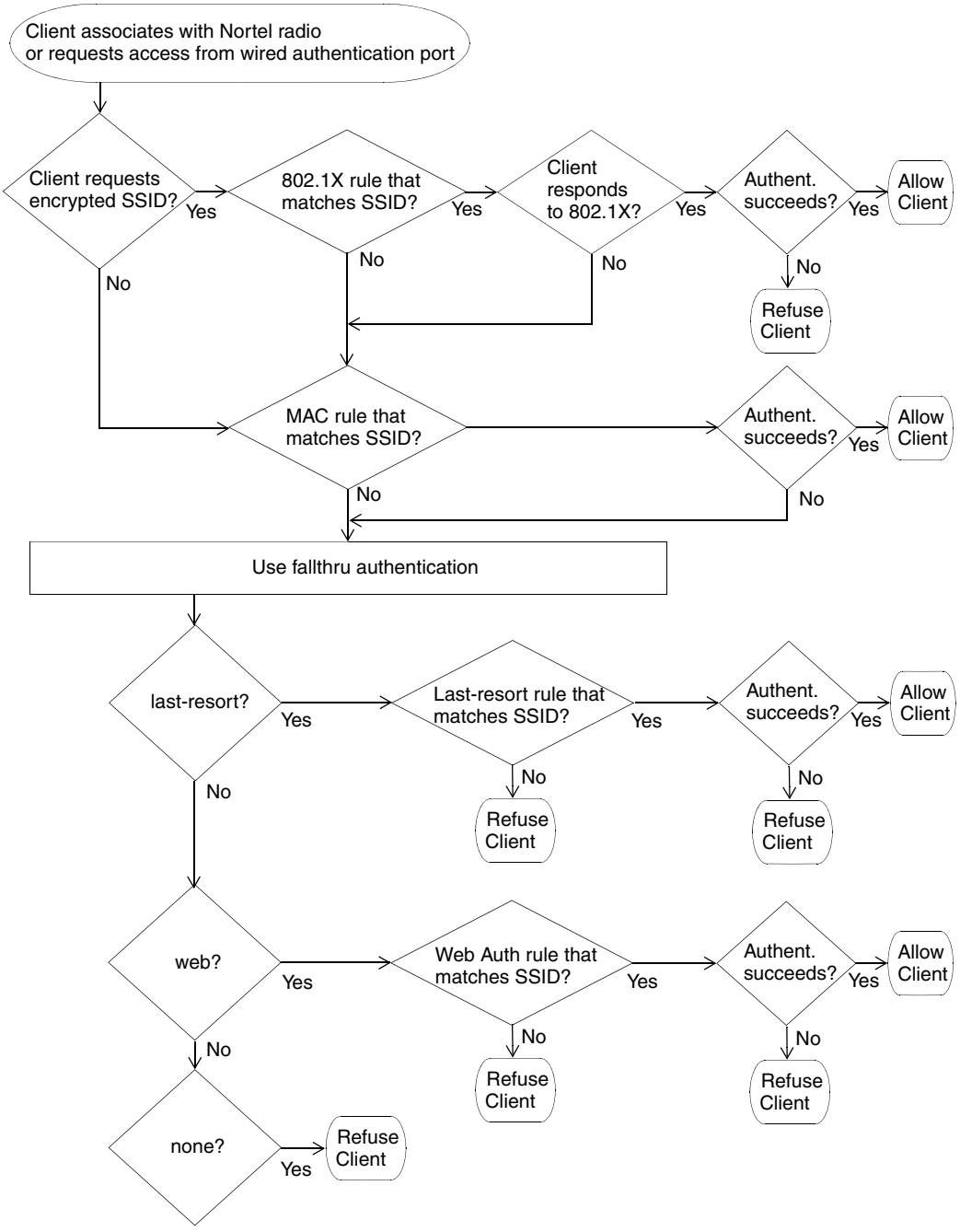
Web and last-resort are described in "Authentication Types". None means the user is automatically denied access. The fallthru authentication type for wireless access is associated with the SSID (through a service profile). The fallthru authentication type for wired authentication access is specified with the wired authentication port. (For information

about service profiles, see “Service Profiles” on page 240. For information about wired authentication port configuration, see “Setting a Port for a Wired Authentication User” on page 76.)

Note. The fallthru authentication type None is different from the authentication method **none** you can specify for administrative access. The fallthru authentication type None denies access to a network user. In contrast, the authentication method **none** allows access to the WSS by an administrator. (See “Configuring AAA for Administrative and Local Access,” on page 51.)

Figure 17 on page 404 shows how WSS Software tries the authentication types.

Figure 17: Authentication Flowchart for Network Users


Client associates with Nortel radio or requests access from wired authentication port
Client requests encrypted SSID?
Yes
No
802.1X rule that matches SSID?
Yes
No
Client responds to 802.1X?
Yes
No
Authent. succeeds?
Yes
No
Allow Client
Refuse Client
MAC rule that matches SSID?
Authent. succeeds?
Yes
No
Allow Client
No
Use fallthru authentication
last-resort?
Yes
No
Last-resort rule that matches SSID?
Yes
No
Refuse Client
Authent. succeeds?
Yes
No
Allow Client
Refuse Client
web?
Yes
No
Web Auth rule that matches SSID?
Yes
No
Refuse Client
Authent. succeeds?
Yes
No
Allow Client
Refuse Client
none?
Yes
Refuse Client

SSID Name "Any"

In authentication rules for wireless access, you can specify the name *any* for the SSID. This value is a wildcard that matches on any SSID string requested by the user.

For 802.1X and Web-based AAA rules that match on SSID *any*, WSS Software checks the RADIUS servers or local database for the username (and password, if applicable) entered by the user. If the user information matches, WSS Software grants access to the SSID requested by the user, regardless of which SSID name it is.

For MAC authentication rules that match on SSID *any*, WSS Software checks the RADIUS servers or local database for the MAC address (and password, if applicable) of the user's device. If the address matches, WSS Software grants access to the SSID requested by the user, regardless of which SSID name it is.

However, in a last-resort authentication rule for wireless access, if the SSID name in the authentication rule is *any*, WSS Software checks the RADIUS servers or local database for username *last-resort-any*, exactly as spelled here. If checking RADIUS, WSS Software also checks for a password. Access is granted only if this username (and password, if applicable) is found. Otherwise, access is denied.

Last-Resort Processing

When a user without a username or password requests wireless access, WSS Software checks the configuration for a last-resort authentication rule that matches on the SSID. If the configuration contains the rule, WSS Software checks the local database for username **last-resort-*ssid***, where ***ssid*** is the SSID requested by the user. The guest user is granted access only if the database or RADIUS server group contains **last-resort-*ssid*** for the SSID requested by the user. Otherwise, access is denied.

This processing of the last-resort username is different from 802.1X, MAC, or Web-based AAA, where WSS Software checks for the exact username or MAC address (and password, if applicable) of the user. WSS Software does not append the SSID to the username (or MAC address) for 802.1X, Web, or MAC authentication.

User Credential Requirements

The user credentials that WSS Software checks for on RADIUS servers or in the local database differ depending on the type of authentication rule that matches on the SSID or wired access requested by the user.

- For a user to be successfully authenticated by an 802.1X or Web-based AAA rule, the username and password entered by the user must be configured on the RADIUS servers used by the authentication rule or in the switch's local database, if the local database is used by the rule.
- For a user to be successfully authenticated based on the MAC address of the user's device, the MAC address must be configured on the RADIUS servers used by the authentication rule or in the switch's local database, if the local database is used by the rule. If the MAC address is configured in the local database, no password is required. However, since RADIUS requires a password, if the MAC address is on the RADIUS server, WSS Software checks for a password. The default well-known password is *Nortel* but is configurable. (The same password applies to last-resort users.)
- For a user to be successfully authenticated for last-resort access, the RADIUS severs or local database (whichever method is used by the last-resort authentication rule), must contain a user named *last-resort-wired* (for wired authentication access) or *last-resort-**ssid***, where ***ssid*** is the SSID requested by the user. If the matching last-resort user is configured in the local database, no password is required. However, since RADIUS requires a password, if the matching last-resort user is on the RADIUS server, WSS Software checks for a password. The default well-known password is *Nortel* but is configurable. (The same password applies to MAC users.)

If the last-resort authentication rule matches on SSID *any*, which is a wildcard that matches on any SSID string, the RADIUS servers or local database must have user *last-resort-any*, exactly as spelled here.

Authorization

If the user is authenticated, WSS Software then checks the RADIUS server or local database (the same place WSS Software looked for user information to authenticate the user) for the authorization attributes assigned to the user. Authorization attributes specify the network resources the user can access.

The only required attribute is the Virtual LAN (VLAN) name on which to place the user. RADIUS and WSS Software have additional optional attributes. For example, you can provide further access controls by specifying the times during which the user can access the network, you can apply inbound and outbound access control lists (ACLs) to the user's traffic, and so on.

To assign attributes on the RADIUS server, use the standard RADIUS attributes supported on the server. To assign attributes in the WSS switch's local database, use the WSS Software vendor-specific attributes (VSAs).

The RADIUS attributes supported by WSS Software are described in "Supported RADIUS Attributes," on page 599.

WSS Software provides the following VSAs, which you can assign to users configured in the local database or on a RADIUS server:

- Encryption-Type—Specifies the type of encryption required for access by the client. Clients who attempt to use an unauthorized encryption method are rejected.
- End-Date—Date and time after which the user is no longer allowed to be on the network.
- Mobility-Profile—Controls the WSS switch ports a user can access. For wireless users, an WSS Software Mobility Profile specifies the AP access ports through which the user can access the network. For wired authentication users, the Mobility Profile specifies the wired authentication ports through which the user can access the network.
- SSID—SSID the user is allowed to access after authentication.
- Start-Date—Date and time at which the user becomes eligible to access the network. WSS Software does not authenticate the user unless the attempt to access the network occurs at or after the specified date and time, but before the end-date (if specified).
- Time-of-Day—Day(s) and time(s) during which the user is permitted to log into the network.
- URL—URL to which the user is redirected after successful Web-based AAA.
- VLAN-Name—VLAN to place the user on.

You also can assign the following RADIUS attributes to users configured in the local database.

- Filter-Id—Security ACL that permits or denies traffic received (input) or sent (output) the WSS switch.
- Service-Type—Type of access the user is requesting, which can be network access, administrative access to the enabled (configuration) mode of the WSS Software CLI, or administrative access to the nonenabled mode of the CLI
- Session-Timeout—Maximum number of seconds allowed for the user's session.

Regardless of whether you configure the user and attributes on RADIUS servers or the switch's local database, the VLAN attribute is required. The other attributes are optional.

Accounting

WSS Software also supports accounting. Accounting collects and sends information used for billing, auditing, and reporting—for example, user identities, connection start and stop times, the number of packets received and sent, and the number of bytes transferred. You can track sessions through accounting information stored locally or on a remote RADIUS server. As network users roam throughout a Mobility Domain, accounting records track them and their network usage.

Summary of AAA Features

Depending on your network configuration, you can configure authentication, authorization, and accounting (AAA) for network users to be performed locally on the WSS switch or remotely on a RADIUS server. The number of users that the local WSS database can support depends on your platform.

AAA for network users controls and monitors their use of the network:

- **Classification for customized access.** As with administrative and console users, you can classify network users through username wildcarding. Based on the structured username, different AAA treatments can be given to different classes of user. For example, users in the human resources department can be authenticated differently from users in the sales department.
- **Authentication for full or limited access.** IEEE 802.1X network users are authenticated when they identify themselves with a credential. Authentication can be passed through to RADIUS, performed locally on the WSS switch, or only partially "offloaded" to the switch. Network users without 802.1X support can be authenticated by the MAC addresses of their devices. If neither 802.1X nor MAC authentication apply to the user, they can still be authenticated by a *fallthru* method, either Web-based AAA or last-resort authentication. Optionally, you can disable the fallthru option by setting the fallthru type to none.
- **Authorization for access control.** Authorization provides access control by means of such mechanisms as per-user security access control lists (ACLs), VLAN membership, Mobility Domain assignment, and timeout enforcement. Because authorization is always performed on network access users so they can use a particular VLAN, the WSS automatically uses the same AAA method (RADIUS server group or local database) for authorization that you define for a user's authentication.
- **Local authorization control.** You can override any AAA assignment of VLAN or security ACL for individual network users on a particular WSS switch by configuring the location policy on the WSS.
- **Accounting for tracking users and resources.** Accounting collects and sends information used for billing, auditing, and reporting—for example, user identities, connection start and stop times, the number of packets received and sent, and the number of bytes transferred. You can track sessions through accounting information stored locally or on a remote RADIUS server. As network users roam throughout a Mobility Domain, accounting records track them and their network usage.

AAA Tools for Network Users

Authentication verifies network user identity and is required before a network user is granted access to the network. An WSS switch authenticates user identity by username-password matching, digital signatures and certificates, or other methods (for example, by MAC address).

You must decide whether to authenticate network users locally on the WSS, remotely through one or more external RADIUS server groups, or both locally and remotely. (For server group details, see "Configuring RADIUS Server Groups" on page 483.)

"Wildcards" and Groups for Network User Classification

"Wildcards" let you classify users by username or MAC address for different AAA treatments. A user wildcard is a string used by AAA and IEEE 802.1X or Web-based AAA methods to match a user or set of users. MAC address wildcards match authentication methods to a MAC address or set of MAC addresses. User wildcards and MAC address wildcards can make use of wildcards. For details, see "User Wildcards, MAC Address Wildcards, and VLAN Wildcards" on page 39.

A user group is a named collection of users or MAC addresses sharing a common authorization policy. For example, you might group all users on the first floor of building 17 into the group *bldg-17-1st-floor*, or group all users in the IT group into the group *infotech-people*.

Wildcard "Any" for SSID Matching

Authentication rules for wireless access include the SSID name, and must match on the SSID name requested by the user for WSS Software to attempt to authenticate the user for that SSID. To make an authentication rule match an any SSID string, specify the SSID name as **any** in the rule.

AAA Methods for IEEE 802.1X and Web Network Access

The following AAA methods are supported by Nortelfor 802.1X and Web network access mode:

- Client certificates issued by a certificate authority (CA) for authentication.

  (For this method, you assign an authentication protocol to a user. For protocol details, see "IEEE 802.1X Extensible Authentication Protocol Types" on page 415.)

- The WSS switch's local database of usernames and user groups for authentication.

  (For configuration details, see "Adding and Clearing Local Users for Administrative Access" on page 63, "Authenticating through a Local Database" on page 420, and "Adding and Clearing MAC Users and User Groups Locally" on page 426.)

- A named group of RADIUS servers. The WSS switch supports up to four server groups, which can each contain between one and four servers.

  (For server group details, see "Configuring RADIUS Server Groups" on page 483.)

You can use the local database or RADIUS servers for MAC and last-resort access as well. If you use RADIUS servers, make sure you configure the password for the MAC address or last-resort user as *nortel*. (This is the default authorization password. To change it, see "Changing the MAC Authorization Password for RADIUS" on page 428.)

AAA Rollover Process

An WSS switch attempts AAA methods in the order in which they are entered in the configuration:

1. The first AAA method in the list is used unless that method results in an error. If the method results in a pass or fail, the result is final and the WSS tries no other methods.
2. If the WSS switch receives no response from the first AAA method, it tries the second method in the list.
3. If the WSS switch receives no response from the second AAA method, it tries the third method. This evaluation process is applied to all methods in the list.



Note. If a AAA rule specifies local as a secondary AAA method, to be used if the RADIUS servers are unavailable, and WSS Software authenticates a client with the local method, WSS Software starts again at the beginning of the method list when attempting to authorize the client. This can cause unexpected delays during client processing and can cause the client to time out before completing logon.

Local Override Exception

The one exception to the operation described in "AAA Rollover Process" takes place if the local database is the *first* method in the list and is followed by a RADIUS server group method. If the local method fails to find a matching

username entry in the local database, the WSS switch tries the next RADIUS server group method. This exception is referred to as local override.

If the local database is the *last* method in the list, however, local authentication must either accept or deny the user, because it has no other method to roll over to.

Remote Authentication with Local Backup

You can use a combination of authentication methods. In pass-through authentication, AAA processing is passed through the WSS switch and performed remotely by RADIUS servers. (For details, see "Using Pass-Through" on page 419.) If RADIUS servers are unavailable, local authentication can take place on the WSS switch.

Suppose an administrator wants to rely on RADIUS servers and also wants to ensure that a certain group of users always gets access. As shown in the following example, the administrator can configure pass-through authentication by a RADIUS server group as the first method for these users and configure local authentication last, in case the RADIUS servers are unavailable. (See Figure 18 on page 414.)

1. To configure *server-1* and *server-2* at IP addresses 192.168.253.1 and 192.168.253.2 with the password *chey3nn3*, the administrator enters the following commands:

   23x0# **set radius server server-1 address 192.168.253.1 key chey3nn3**

   23x0# **set radius server server-2 address 192.168.253.2 key chey3nn3**

2. To configure *server-1* and *server-2* into *server-group-1*, the administrator enters the following command:

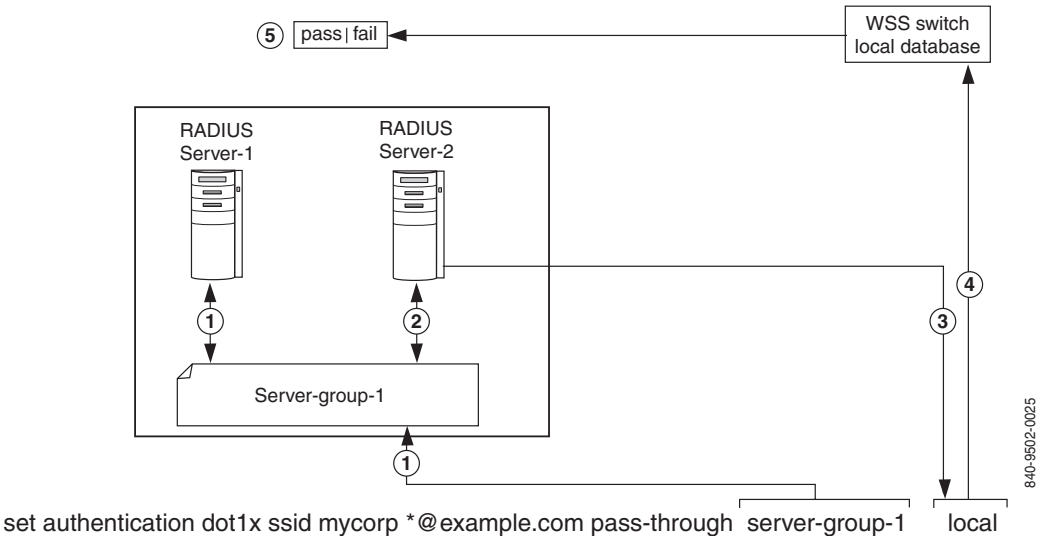
   23x0# **set server group server-group-1 members server-1 server-2**

3. To enable pass-through plus local authentication for all users of SSID *mycorp* at @example.com, the administrator enters the following command.

   23x0# **set authentication dot1x ssid mycorp *@example.com pass-through server-group-1 local**

Figure 18 on page 414 shows the results of this combination of methods.

Figure 18: Remote Pass-Through or Local Authentication



Authentication proceeds as follows:

1. When user Jose@example.com attempts authentication, the WSS switch sends an authentication request to the first AAA method, which is *server-group-1*.

   Because *server-group-1* contains two servers, the first RADIUS server, *server-1*, is contacted. If this server responds, the authentication proceeds using *server-1*.

2. If *server-1* fails to respond, the WSS retries the authentication using *server-2*. If *server-2* responds, the authentication proceeds using *server-2*.

3. If *server-2* does not respond, because the WSS switch has no more servers to try in *server-group-1*, the WSS attempts to authenticate using the next AAA method, which is the *local* method.

4. The WSS switch consults its local database for an entry that matches Jose@example.com.

5. If a suitable local database entry exists, the authentication proceeds. If not, authentication fails and Jose@example.com is not allowed to access the network.

IEEE 802.1X Extensible Authentication Protocol Types

Extensible Authentication Protocol (EAP) is a generic point-to-point protocol that supports multiple authentication mechanisms. EAP has been adopted as a standard by the Institute of Electrical and Electronic Engineers (IEEE). IEEE 802.1X is an encapsulated form for carrying authentication messages in a standard message exchange between a user (client) and an authenticator.

Table 28 on page 415 summarizes the EAP protocols (also called types or methods) supported by WSS Software.

Table 28: EAP Authentication Protocols for Local Processing

EAP Type	Description	Use	Considerations
EAP-MD5 (EAP with Message Digest Algorithm 5)	Authentication algorithm that uses a challenge-response mechanism to compare hashes	Wired authentication only1	This protocol provides no encryption or key establishment.
EAP-TLS (EAP with Transport Layer Security)	Protocol that provides mutual authentication, integrity-protected encryption algorithm negotiation, and key exchange. EAP-TLS provides encryption and data integrity checking for the connection.	Wireless and wired authentication. All authentication is processed on the WSS switch.	This protocol requires X.509 public key certificates on both sides of the connection.
PEAP-MS-CHAP-V2 (Protected EAP with Microsoft Challenge Handshake Authentication Protocol version 2)	The wireless client authenticates the server (either the WSS switch or a RADIUS server) using TLS to set up an encrypted session. Mutual authentication is performed by MS-CHAP-V2.	Wireless and wired authentication: • The PEAP portion is processed on the WSS switch. • The MS-CHAP-V2 portion is processed on the RADIUS server or locally, depending on the configuration.	Only the server side of the connection requires a certificate. The client needs only a username and password.

1. EAP-MD5 does not work with Microsoft wired authentication clients.

Ways an WSS Switch Can Use EAP

Network users with 802.1X support cannot access the network unless they are authenticated. You can configure an WSS switch to authenticate users with EAP on a group of RADIUS servers and/or in a local user database on the WSS, or to offload some authentication tasks from the server group. Table 29 on page 416 details these three basic WSS authentication approaches.

(For information about digital certificates, see "Managing Keys and Certificates," on page 379.)

Table 29: Three Basic WSS Approaches to EAP Authentication

Approach	Description
Pass-through	An EAP session is established directly between the client and RADIUS server, passing through the WSS switch. User information resides on the server. All authentication information and certificate exchanges pass through the switch or use client certificates issued by a certificate authority (CA). In this case, the switch does not need a digital certificate, although the client might.
Local	The WSS switch performs all authentication using information in a local user database configured on the switch, or using a client-supplied certificate. No RADIUS servers are required. In this case, the switch needs a digital certificate. If you plan to use the EAP with Transport Layer Security (EAP-TLS) authentication protocol, the clients also need certificates.
Offload	The WSS switch offloads all EAP processing from a RADIUS server by establishing a TLS session between the switch and the client. In this case, the switch needs a digital certificate. If you plan to use the EAP-TLS authentication protocol, the clients also need certificates. When you use offload, RADIUS can still be used for non-EAP authentication and authorization.

Effects of Authentication Type on Encryption Method

Wireless users who are authenticated on an encrypted service set identifier (SSID) can have their data traffic encrypted by the following methods:

- Wi-Fi Protected Access (WPA) encryption
- Non-WPA dynamic Wired Equivalent Privacy (WEP) encryption
- Non-WPA static WEP encryption

(For encryption details, see "Configuring User Encryption," on page 191.)

The authentication method you assign to a user determines the encryption available to the user. Users configured for EAP authentication, MAC authentication, Web, or last-resort authentication can have their traffic encrypted as follows:

EAP Authentication	MAC Authentication	Last-Resort Authentication	Web-based AAA
WPA encryption	Static WEP	Static WEP	Static WEP
Dynamic WEP encryption	No encryption (if SSID is unencrypted)	No encryption (if SSID is unencrypted)	No encryption (if SSID is unencrypted)

Wired users are not eligible for the encryption performed on the traffic of wireless users, but they can be authenticated by an EAP method, a MAC address, a Web login page served by the WSS switch, or a last-resort username.

Configuring 802.1X Authentication

The IEEE 802.1X standard is a framework for passing EAP protocols over a wired or wireless LAN. Within this framework, you can use TLS, PEAP-TTLS, or EAP-MD5. Most EAP protocols can be passed through the WSS switch to the RADIUS server. Some protocols can be processed locally on the WSS switch.

The following 802.1X authentication command allows differing authentication treatments for multiple users:

set authentication dot1x {**ssid** *ssid-name* | **wired**} *user-wildcard* [**bonded**] *protocol method1* [*method2*] [*method3*] [*method4*]

For example, the following command authenticates wireless user *Tamara*, when requesting SSID *wetlands*, as an 802.1X user using the PEAP-MS-CHAP-V2 method through the server group *shorebirds*, which contains one or more RADIUS servers:

```
23x0# set authentication dot1x ssid wetlands Tamara peap-mschapv2 shorebirds
```

When a user attempts to connect through 802.1X, the following events occur:

1. For each 802.1X login attempt, WSS Software examines each command in the configuration file in strict configuration order.
2. The first command whose SSID and user wildcard matches the SSID and incoming username is used to process this authentication. The command determines exactly how this particular login attempt is processed by the WSS switch.

(For more information about user wildcards, see "User Wildcards" on page 39.)

Configuring 802.1X Acceleration

You can configure the WSS switch to offload all EAP processing from server groups. In this case, the RADIUS server is not required to communicate using the EAP protocols.

For PEAP-MS-CHAP-V2 offload, you define a complete user profile in the local WSS database and only a username and password on a RADIUS server. For EAP-TLS offload, you define a complete user profile in the local database only.

For example, the following command authenticates all wireless users who request SSID *marshes* at example.com by offloading PEAP processing onto the WSS switch, while still performing MS-CHAP-V2 authentication through the server group *shorebirds*:

```
23x0# set authentication dot1x ssid marshes *@example.com peap-mschapv2 shorebirds
```

To offload *both* PEAP and MS-CHAP-V2 processing onto the WSS switch, use the following command:

```
23x0# set authentication dot1x ssid marshes *@example.com peap-mschapv2 local
```

Using Pass-Through

The pass-through method causes EAP authentication requests to be processed entirely by remote RADIUS servers in server groups.

For example, the following command enables users at EXAMPLE to be processed through server group *shorebirds* or *swampbirds*:

```
23x0# set authentication dot1X ssid marshes EXAMPLE/* pass-through shorebirds
      swampbirds
```

The server group *swampbirds* is contacted only if all the RADIUS servers in *shorebirds* do not respond.

(For an example of the use of pass-through servers plus the local database for authentication, see "Remote Authentication with Local Backup" on page 413.)

Authenticating through a Local Database

To configure the WSS switch to authenticate and authorize a user against the local database in the WSS switch, use the following command:

set authentication dot1x {ssid *ssid-name* **| wired}** *user-wildcard* **[bonded]** *protocol* **local**

For example, the following command authenticates 802.1X user *Jose* for wired authentication access through the local database:

```
2370# set authentication dot1X Jose wired peap-mschapv2 local
success: change accepted.
```

Binding User Authentication to Machine Authentication

Bonded Authentication™ (bonded authentication) is a security feature that binds an 802.1X user's authentication to authentication of the machine from which the user is attempting to log on. When this feature is enabled, WSS Software authenticates a user only if the machine from which the user logs on has already been authenticated separately.

By default, WSS Software does not bind user authentication to machine authentication. A trusted user can log on from any machine attached to the network.

You can use Bonded Authentication with Microsoft Windows clients that support separate 802.1X authentication for the machine itself and for a user who uses the machine to log on to the network.

Network administrators sometimes use machine authentication in a Microsoft Active Directory domain to run login scripts, and to control defaults, application access and updates, and so on. Bonded Authentication provides an added security measure, by ensuring that a trusted user can log onto the network only from a trusted machine known to Active Directory.

For example, if user bob.mycorp.com has a trusted laptop PC used for work but also has a personal laptop PC, you might want to bind Bob's authentication with the authentication of his workplace laptop, host/bob-laptop.mycorp.com. In this case, Bob can log on to the company network only from his work laptop.

When Bonded Authentication is enabled, WSS Software retains information about the machine's session when a user logs on from that machine. WSS Software authenticates the user only if there has already been a successful machine authentication. Evidence of the machine's session in WSS Software indicates that the machine has successfully authenticated and is therefore trusted by WSS Software. If WSS Software does not have session information for the machine,

WSS Software refuses to authenticate the user and does not allow the user onto the network from the unauthenticated machine.



Note. If the 802.1X reauthentication parameter or the RADIUS Session-Timeout parameter is applicable, the user must log in before the 802.1X reauthentication timeout or the RADIUS session-timeout for the machine's session expires. Normally, these parameters apply only to clients that use dynamic WEP, or use WEP-40 or WEP-104 encryption with WPA or RSN.

Authentication Rule Requirements

Bonded Authentication requires an 802.1X authentication rule for the machine itself, and a separate 802.1X authentication rule for the user(s). Use the **bonded** option in the user authentication rule, but not in the machine authentication rule.

The authentication rule for the machine must be higher up in the list of authentication rules than the authentication rule for the user.

You must use 802.1X authentication rules. The 802.1X authentication rule for the machine must use **pass-through** as the protocol. Nortel recommends that you also use **pass-through** for the user's authentication rule.

The rule for the machine and the rule for the user must use a RADIUS server group as the method. (Generally, in a Bonded Authentication configuration, the RADIUS servers will use a user database stored on an Active Directory server.)

(For a configuration example, see "Bonded Authentication Configuration Example" on page 423.)

Nortel recommends that you make the rules as general as possible. For example, if the Active Directory domain is mycorp.com, the following userwildcards match on all machine names and users in the domain:

- host/*.mycorp.com (userwildcard for the machine authentication rule)
- *.mycorp.com (userwildcard for the user authentication rule)

If the domain name has more nodes (for example, nl.mycorp.com), use an asterisk in each node that you want to match globally. For example, to match on all machines and users in mycorp.com, use the following userwildcards:

- host/*.*.mycorp.com (userwildcard for the machine authentication rule)
- *.*.mycorp.com (userwildcard for the user authentication rule)

Use more specific rules to direct machines and users to different server groups. For example, to direct users in nl.mycorp.com to a different server group than users in de.mycorp.com, use the following userwildcards:

- host/*.nl.mycorp.com (userwildcard for the machine authentication rule)
- *.nl.mycorp.com (userwildcard for the user authentication rule)
- host/*.de.mycorp.com (userwildcard for the machine authentication rule)
- *.de.mycorp.com (userwildcard for the user authentication rule)

Bonded Authentication Period

The *Bonded Authentication period* is the number of seconds WSS Software allows a Bonded Authentication user to reauthenticate.

After successful machine authentication, a session for the machine appears in the session table in WSS Software. When the user logs on and is authenticated, the user session replaces the machine session in the table. However, since the user's authentication rule contains the **bonded** option, WSS Software remembers that the machine was authenticated.

If a Bonded Authentication user's session is ended due to 802.1X reauthentication or the RADIUS Session-Timeout parameter, WSS Software can allow time for the user to reauthenticate. The amount of time that WSS Software allows for reauthentication is controlled by the Bonded Authentication period.

If the user does not reauthenticate within the Bonded Authentication period, WSS Software deletes the information about the machine session. After the machine session information is deleted, the Bonded Authentication user cannot reauthenticate. When this occurs, the user will need to log off, then log back on, to access the network. After multiple failed reauthentication attempts, the user might need to reboot the PC before logging on.

By default, the Bonded Authentication period is 0 seconds. WSS Software does not wait for a Bonded Authentication user to reauthenticate.

You can set the Bonded Authentication period to a value up to 300 seconds. Nortel recommends that you try 60 seconds, and change the period to a longer value only if clients are unable to authenticate within 60 seconds.

To set the Bonded Authentication period, use the following command:

set dot1x bonded-period *seconds*

To reset the Bonded Authentication period to its default value (0), use the following command:

clear dot1x bonded-period

Bonded Authentication Configuration Example

To configure Bonded Authentication:

- Configure separate authentication rules for the machine and for the user(s).
- Set the Bonded Authentication period.
- Verify the configuration changes.

The following commands configure two 802.1X authentication rules for access to SSID *mycorp*. The first rule is for authentication of all trusted laptop PCs at mycorp.com (host/*-laptop.mycorp.com). The second rule is

for bonded authentication of all users at mycorp.com (*.mycorp.com). Both rules use pass-through as the protocol, and use RADIUS server group *radgrp1*.

```
23x0# set authentication dot1x ssid mycorp host/*-laptop.mycorp.com pass-through radgrp1
success: change accepted.

23x0# set authentication dot1x ssid mycorp  *.mycorp.com  bonded pass-through radgrp1
success: change accepted.
```

The following command sets the Bonded Authentication period to 60 seconds, to allow time for WEP users to reauthenticate:

```
23x0# set dot1x bonded-period 60
success: change accepted.
```

Displaying Bonded Authentication Configuration Information

To display Bonded Authentication configuration information, use the following command:

show dot1x config

In the following example, bob.mycorp.com uses Bonded Authentication, and the Bonded Authentication period is set to 60 seconds.

```
23x0# show dot1x config

              802.1X user policy
            ----------------------
'host/bob-laptop.mycorp.com' on ssid 'mycorp' doing PASSTHRU
'bob.mycorp.com' on ssid 'mycorp' doing PASSTHRU (bonded)

802.1X parameter               setting
----------------               -------
supplicant timeout             30
auth-server timeout            30
quiet period                   60
transmit period                5
reauthentication period        3600
maximum requests               2
key transmission               enabled
reauthentication               enabled
authentication control         enabled
WEP rekey period               1800
WEP rekey                      enabled
Bonded period                  60
```

Information for the 802.1X authentication rule for the machine (host/bob-laptop.mycorp.com) is also displayed. However, the **bonded** option is configured only for the user's authentication rule. The **bonded** option applies only to the authentication rules for users, not the authentication rules for machines.

Configuring Authentication and Authorization by MAC Address

You must sometimes authenticate users based on the MAC addresses of their devices rather than a username-password or certificate. For example, some Voice-over-IP (VoIP) phones and personal digital assistants (PDAs) do not support 802.1X authentication. If a client does not support 802.1X, WSS Software attempts to perform MAC authentication for the client instead. The WSS can discover the MAC address of the device from received frames and can use the MAC address in place of a username for the client.

Users authorized by MAC address require a MAC authorization password if RADIUS authentication is desired. The default well-known password is *nortel*.



Caution! Use this method with care. IEEE 802.11 frames can be forged and can result in unauthorized network access if MAC authentication is employed.

Adding and Clearing MAC Users and User Groups Locally

MAC users and groups can gain network access only *through* the WSS switch. They cannot create administrative connections *to* the WSS switch. A MAC user is created in a similar fashion to other local users except for having a MAC address instead of a username. MAC user groups are created in a similar fashion to other local user groups.

(To create a MAC user profile or MAC user group on a RADIUS server, see the documentation for your RADIUS server.)

Adding MAC Users and Groups

To create a MAC user group in the local WSS database, you must associate it with an authorization attribute and value. Use the following command:

set mac-usergroup *group-name* **attr** *attribute-name value*

For example, to create a MAC user group called *mac-easters* with a 3000-second Session-Timeout value, type the following command:

```
23x0# set mac-usergroup mac-easters attr session-timeout 3000
success: change accepted.
```

To configure a MAC user in the local database and optionally add the user to a group, use the following command:

set mac-user *mac-addr* [**group** *group-name*]

For example, type the following command to add MAC user 01:0f:03:04:05:06 to group *macfans:*

```
23x0# set mac-user 01:0f:03:04:05:06 group macfans
success: change accepted.
```

Clearing MAC Users and Groups

To clear a MAC user from a user group, use the following command:

clear mac-user *mac-addr* **group**

For example, the following command removes MAC user 01:0f:03:04:05:06 from group *macfans:*

```
23x0# clear mac-user 01:0f:03:04:05:06 group
success: change accepted.
```

The **clear mac-usergroup** command removes the group.

To remove a MAC user profile from the local database on the WSS switch, type the following command:

clear mac-user *mac-address*

For example, the following command removes MAC user 01:0f:03:04:05:06 from the local database:

```
23x0# clear mac-user 01:0f:03:04:05:06
success: change accepted.
```

Configuring MAC Authentication and Authorization

The **set authentication mac** command defines the AAA methods by which MAC addresses can be used for authentication. You can configure authentication for users through the MAC addresses of their devices with the following command:

set authentication mac {**ssid** *ssid-name* | **wired**} *mac-addr-wildcard method1* [*method2*] [*method3*] [*method4*]

MAC addresses can be authenticated by either the WSS switch's local database or by a RADIUS server group. For example, the following command sets the authentication for MAC address 01:01:02:03:04:05 when requesting SSID *voice*, through the local database:

```
23x0# set authentication mac ssid voice 01:01:02:03:04:05 local
success: change accepted
```

If the switch's configuration does not contain a **set authentication mac** command that matches a non-802.1X client's MAC address, WSS Software tries MAC authentication by default.

You can also wildcard MAC addresses. For example, the following command locally authenticates all MAC addresses that begin with the octets 01:01:02:

```
23x0# set authentication mac ssid voice 01:01:02:* local
success: change accepted
```

(For details about MAC address wildcards, see "MAC Address Wildcards" on page 39.)

You can add authorization attributes to authenticated MAC users with the following command:

set mac-user *mac-addr* **attr** *attribute-name value*

For example, to add the MAC user 00:01:02:03:04:05 to VLAN *red*:

```
23x0# set mac-user 00:01:02:03:04:05 attr vlan-name red
success: change accepted
```

To change the value of an authorization attribute, reenter the command with the new value. To clear an authorization attribute from a MAC user profile in the local database, use the following command:

clear mac-user *mac-addr* **attr** *attribute-name*

For example, the following command clears the VLAN assignment from MAC user 01:0f:02:03:04:05:

```
23x0# clear mac-user 01:0f:03:04:05:06 attr vlan-name
success: change accepted.
```

(For a complete list of authorization attributes, see Table 32 on page 446.)

Changing the MAC Authorization Password for RADIUS

When you enable MAC authentication, the client does not supply a regular username or password. The MAC address of the user's device is extracted from frames received from the device.

To authenticate and authorize MAC users through RADIUS, you must configure a single predefined password for MAC users, which is called the outbound authorization password. The same password is used for all MAC user entries in the RADIUS database. Set this password by typing the following command:

set radius server *server-name* **author-password** *password*

The default password is *nortel*.

Note. Before setting the outbound authorization password for a RADIUS server, you must have set the address for the RADIUS server. For more information, see "Configuring RADIUS Servers" on page 479.

For example, the following command sets the outbound authorization password for MAC users on server *bigbird* to *h00per*:

```
23x0# set radius server bigbird author-password h00per
success: change accepted.
```

Note. A MAC address must be dash-delimited in the RADIUS database—for example, 00-00-01-03-04-05. However, the WSS Software always displays colon-delimited MAC addresses.

If the MAC address is in the database, WSS Software uses the VLAN attribute and other attributes associated with it for user authorization. Otherwise, WSS Software tries the fallthru authentication type, which can be last-resort, Web, or none.

Configuring Web-based AAA

Web-based AAA simplifies secure access to unencrypted SSIDs. When a user requests access to an SSID or attempts to access a web page before logging onto the network, WSS Software serves a login page to the user's browser. After the user enters a username and password, WSS Software checks the local database or RADIUS servers for the user information, and grants or denies access based on whether the user information is found.

WSS Software redirects an authenticated user back to the requested web page, or to a page specified by the administrator.

Web-based AAA, like other types of authentication, is based on an SSID or on a wired authentication port.

WSS Software provides a Nortel login page, which is used by default. You can add custom login pages to the WSS switch's nonvolatile storage, and configure WSS Software to serve those pages instead.

Web-based AAA is the default fallthru authentication type for wireless access.

How Portal Web-based AAA Works

1. A Web-based AAA user attempts to access the network. For a wireless user, this begins when the user's network interface card (NIC) associates with an SSID on a Nortel radio. For a wired authentication user, this begins when the user's NIC sends data on the wired authentication port.
2. The user opens a web browser. The web browser sends a DNS request for the IP address of the home page or a URL requested by the user.
3. If user **web-portal-*ssid*** has been configured for the SSID (or **web-portal-wired**, if the user is on a wired authentication port), WSS Software does the following:
   - Intercepts the DNS request, uses the WSS Software DNS proxy to obtain the URL's IP address from the network DNS server, and sends the address to the user's browser.
   - Serves a login page to the Web-based AAA user.

   The **web-portal-*ssid*** and **web-portal-wired** users allow temporary access to limited network resources (by default, DHCP only) while WSS Software authenticates and authorizes the Web-based AAA user. The access to DHCP allows the user to obtain an IP configuration while WSS Software is authenticating and authorizing the user.
4. The user enters their username and password in the Web-based AAA login page.
5. WSS Software starts a portal session for the user and places the user in the VLAN associated with the **web-portal-*ssid*** or **web-portal-wired** user. A portal session allows the user to obtain an IP configuration while WSS Software authenticates and authorizes the user. WSS Software authenticates the user by checking RADIUS or the switch's local database for the username and password entered by the user. If the user information is present, WSS Software authorizes the user based on the authorization attributes set for the user.



Note. WSS Software ignores the VLAN-Name or Tunnel-Private-Group-ID attribute associated with the user, and leaves the user in the VLAN associated with the **web-portal-*ssid*** or **web-portal-wired** user. When you configure **web-portal-*ssid*** or **web-portal-wired** users, make sure you associate them with the VLAN in which you want to place authorized Web-based AAA users.

6. After authentication and authorization are complete, WSS Software changes the user's session from a portal session with the name **web-portal-*ssid*** or **web-portal-wired** to a Web-based AAA session with the user's name. The session remains connected, but is now an identity-based session for the user instead of a portal session.
7. WSS Software redirects the browser to the URL initially requested by the user or, if the URL VSA is configured for the user, redirects the user to the URL specified by the VSA.
8. The web page for the URL to which the user is redirected appears in the user's browser window.

Web-based AAA Requirements and Recommendations

WSS Requirements

- Web-based AAA certificate—You must install a Web-based AAA certificate on the switch. You can install a certificate signed by a trusted third-party certificate authority (CA), or one signed by the WSS switch itself. (For information, see "Managing Keys and Certificates," on page 379 or the *Nortel Wireless Security Switch Installation and Basic Configuration Guide*.)
- If you choose to install a self-signed Web-based AAA certificate, use a common name (a required field in the certificate), that resembles a web address and contains at least one dot. When WSS Software serves the login page to the browser, the page's URL is based on the common name in the Web-based AAA certificate.

  Here are some examples of common names in the recommended format:

  - webaaa.login
  - webaaa.customername.com
  - webaaa.local

  Here are some examples of common names that are not in the recommended format:

  - webaaa
  - trpz_webaaa
  - web
- DNS must be configured. Configure the primary DNS server, and secondary servers if applicable (**set ip dns server** command). Also configure the default domain name (**set ip dns domain** command), and enable DNS (**set ip dns enable** command). By default, DNS is disabled and none of its parameters are configured.
- User VLAN—The user's VLAN must be statically configured on the WSS switch, and an IP interface must be configured on the VLAN. The interface must be in the subnet on which the DHCP server will place the user. (To configure a VLAN, see "Configuring and Managing VLANs" on page 88.)
- Fallthru authentication type—The fallthru authentication type for each SSID and wired authentication port that you want to support Web-based AAA, must be set to **web-portal**. This is the default fallthru authentication type for SSIDs but not for wired authentication ports.

  To set the fallthru authentication type for an SSID, set it in the service profile for the SSID, using the **set service-profile auth-fallthru** command. To set it on a wired authentication port, use the **auth-fall-thru web-portal** parameter of the **set port type wired-auth** command.
- Portal users—For each SSID, a **web-portal-*ssid*** user must be configured, and the VLAN-Name and Filter-Id attributes must be configured. The VLAN-Name attribute must be set to the VLAN on which you want to place users of the SSID. The Filter-Id attribute must map the ACL *web* to the **web-portal-*ssid*** user, on the inbound traffic direction. (The name *web* is the default name of the ACL created for portal Web-based AAA.)

  You can create the **web-portal-*ssid*** user in the local database, on RADIUS servers, or both. A Web-based AAA authentication rule can use either or both of these authentication and authorization methods.

The *web* ACL is created automatically by WSS Software, and has the following ACEs:

set security acl ip portalacl.in permit udp 0.0.0.0 255.255.255.255 eq 68 0.0.0.0 255.255.255.255 eq 67

set security acl ip portalacl.in deny 0.0.0.0 255.255.255.255 capture



Caution! If you do not use the Filter-Id attribute to map the portal ACL to the inbound traffic direction of the **web-portal-*ssid*** and **web-portal-wired** users, the Web-based AAA users are placed into the VLAN associated with the **web-portal-*ssid*** or **web-portal-wired** user, without any filters.

For wired authentication ports, create a **web-portal-wired** user and configure the VLAN-Name and Filter-Id attributes as described above. The VLAN-Name must be the user's VLAN and the Filter-Id attribute must map the *web* ACL created by WSS Software to the inbound traffic direction.



Note. Portal Web-based AAA does not assign a user to a VLAN based on the VLAN-Name or Tunnel-Private-Group-ID authorization attribute set for the user. WSS Software ignores these attributes and leaves the user in the VLAN assigned to the **web-portal-*ssid*** or **web-portal-wired** user.

- Web-based AAA users—Information for the username that will be entered for login must be configured in the local database or on a RADIUS server. You can configure authorization attributes for the Web-based AAA user. However, the VLAN-Name or Tunnel-Private-Group-ID attribute is ignored. The optional VSAs include **url**, which redirects an authenticated user to a URL other than the one they were attempting to access when they logged on.

  To configure user information in the local database, use the **set user** and **set user** *username* **attr** commands. To configure user groups and set attributes on a group basis, use the **set user** *username* **group** and **set usergroup** commands.

- Authentication rules—A last-resort authentication rule must be configured for each **web-portal-*ssid*** user and the **web-portal-wired** user, if configured. The last-resort rule specifies the authentication method (local database or RADIUS server group) to use for the part of the session during which the user is waiting to be authenticated and authorized.

  In addition, a web authentication rule must be configured for the Web-based AAA users. Whereas the last-resort rule matches on the **web-portal-*ssid*** or **web-portal-wired** user, the web rule must match on the username the Web-based AAA user will enter on the Web-based AAA login page. The web rule also must match on the SSID the user will use to access the network. If the user will access the network on a wired authentication port, the rule must match on **wired**.

  To configure authentication rules, use the **set authentication web** and **set authentication last-resort** commands.

- Portal Web-based AAA must be enabled, using the **set web-aaa** command. The feature is enabled by default.

Portal ACL and User ACLs

The ACL that WSS Software creates automatically for the **web-portal-*ssid*** and **web-portal-wired** users applies only when a user's session is in the portal state. After the user is authenticated and authorized, the ACL is no longer applicable.

To modify a user's access while the user is still being authenticated and authorized, modify the ACL mapped to the **web-portal-*ssid*** or **web-portal-wired** user. To modify a Web-based AAA user's access after the user is authenticated and authorized, map an ACL to the individual Web-based AAA user. Changes you make to the ACL mapped to the **web-portal-*ssid*** or **web-portal-wired** user do not affect user access after authentication and authorization are complete.

You do not need to make any configuration changes to the portal ACL. However, you can add ACEs to it if desired. For example, if you want to allow the user to access a credit card server while WSS Software is still authenticating and authorizing the user, you can add a permit ACE to the portal ACL. Do not change the ACEs that are already in the ACL, and make sure the last ACE in the ACL is the deny ACE that captures all traffic.

WSS Recommendations

- Consider installing a Web-based AAA certificate signed by a trusted CA, instead of one signed by the WSS switch itself. Unless the client's browser is configured to trust the signature on the switch's Web-based AAA certificate, display of the login page can take several seconds longer than usual, and might be interrupted by a dialog asking the user what to do about the untrusted certificate. Generally, the browser is already configured to trust certificates signed by a CA.
- Do not configure the service profile that manages the SSID to use WPA encryption with pre-shared keys (PSK). These options are configurable together but are not compatible. Web-based AAA traffic is not encrypted, whereas the PSK four-way handshake requires a client to already be authenticated and for encryption to be in place.

Client NIC Requirements

- Configure the NIC to use DHCP to obtain its IP address. Web-based AAA does not support statically assigned IP addresses.

Client Web Browser Requirements

- Do not configure an HTTPS proxy. Web-based AAA does not work if the browser has an HTTPS proxy enabled.

Client Web Browser Recommendations

- Use a well-known browser, such as Internet Explorer (Windows), Firefox (Mozilla-based), or Safari (Macintosh)
- If the Web-based AAA certificate on the WSS switch is self-signed, configure the browser to trust the signature by installing the certificate on the browser, so that the browser does not display a dialog about the certificate each time the user tries to log on.

Configuring Portal Web-based AAA

To configure portal Web-based AAA:

1. Configure the user's VLAN on the WSS switch, and configure an IP interface on the VLAN.The interface must be in the subnet on which the DHCP server will place the user.
2. Set the fallthru authentication type to **web-portal** for all SSIDs and wired authentication ports through which Web-based AAA users will access the network. The default for SSIDs is already **web-portal**. However, the default for wired authentication ports is **none**.
3. Configure **web-portal-*ssid*** and **web-portal-wired** users. You must create a **web-portal-*ssid*** user for each SSID. However, the **web-portal-wired** user is applicable to all wired authentication ports.

   Set the VLAN-Name and Filter-Id attributes for these users. For the VLAN-Name, specify the VLAN in which you want to place authorized Web-based AAA users. For Filter-Id, specify the portal ACL, and map the ACL to the inbound traffic direction.
4. Configure individual Web-based AAA users. Because the VLAN is assigned based on the **web-portal-*ssid*** or **web-portal-wired** user, WSS Software ignores the VLAN-Name and Tunnel-Private-Group-ID attributes. However, WSS Software does assign other attributes if set.
5. Configure a last-resort authentication rule for each **web-portal-*ssid*** and **web-portal-wired** user.
6. Configure web authentication rules for the Web-based AAA users.
7. Save the configuration changes.

Portal Web-based AAA Configuration Example

This example configures portal Web-based AAA for wireless users of SSID *mycorp*. The **web-portal-mycorp** user and the individual Web-based AAA users are configured in the local database. The default fallthru authentication type for SSIDs is already **web-portal**, so this example does not include the command to set it.

1. Configure the user's VLAN on ports 2 and 3, and configure an IP interface on the VLAN:

   23x0# **set vlan corpvlan port 2-3**
   success: change accepted.

   23x0# **set interface corpvlan ip 192.168.12.10 255.255.255.0**
   success: change accepted.
2. Configure user **web-portal-mycorp** for SSID *mycorp*, which Web-based AAA users will use to access the network. Use the **vlan-name** attribute to assign the user to the VLAN *corpvlan*.

   23x0# **set user web-portal-mycorp attr vlan-name corpvlan**
3. Assign the ACL *web* to the inbound traffic direction for user **web-portal-mycorp**:

   23x0# **set user web-portal-mycorp attr filter-id portalacl.in**
4. Configure individual Web-based AAA users.

   23x0# **set user alice password alicepword**
   success: change accepted.

   23x0# **set user bob password bobpword**
   success: change accepted.

5 Configure a last-resort authentication rule for user **web-portal-mycorp**:

```
23x0# set authentication last-resort ssid mycorp local
success: change accepted.
```

6 Configure a web authentication rule for Web-based AAA users:

```
23x0# set authentication portalacl.in ssid mycorp ** local
success: change accepted.
```

7 Display the configuration:

```
23x0# show config
# Configuration nvgen'd at 2005-5-09 19:14:10
# Image 4.0.1
# Model WSS-2360
# Last change occurred at 2005-5-09 19:13:45
...
set authentication last-resort ssid mycorp local
set authentication portalacl.in ssid mycorp ** local
set user web-portal-mycorp attr vlan-name corpvlan
set user web-portal-mycorp attr filter-id portalacl.in
set user alice password alicepword
set user bob password bobpword
...
set vlan corpvlan port 2-3
set interface corpvlan ip 192.168.12.10 255.255.255.0
...
set security acl ip portalacl.in permit udp 0.0.0.0
255.255.255.255 eq 68 0.0.0.0 255.255.255.255 eq
   67
set security acl ip portalacl.in deny 0.0.0.0 255.255.255.255
capture
commit security acl portalacl.in
```

8 Save the configuration changes:

```
23x0# save config
success: configuration saved.
```

Displaying Session Information for Portal Web-based AAA Users

To display user session information for portal Web-based AAA users, use the following command:

show sessions network [user *user-wildcard* | **mac-addr** *mac-addr-wildcard* | **ssid** *ssid-name* | **vlan** *vlan-wildcard* | **session-id** *session-id* | **wired] [verbose]**

You can determine whether a portal Web-based AAA user has completed the authentication and authorization process, based on the username displayed in the session table. The following command shows the sessions for SSID *mycorp*.

```
23x0# show sessions network ssid mycorp
User                          Sess  IP or MAC         VLAN            Port/
Name                            ID  Address           Name            Radio
----------------------------- ----  ----------------- --------------- -----
```

```
alice                              4* 192.168.12.101    corpvlan          3/1
web-portal-mycorp                  5  192.168.12.102    corpvlan          3/1
2 sessions total
```

This example shows two sessions. The session for *alice* has the user's name and is flagged with an asterisk (*). The asterisk indicates that the user has completed authentication and authorization. The session for **web-portal-mycorp** indicates that a Web-based AAA user is on the network but is still being authenticated. The user *alice* has all the access privileges configured for the user, whereas the user who is still on the portal session with the name **web-portal-mycorp** has limited access to resources. By default, this user can send and receive DHCP traffic only.

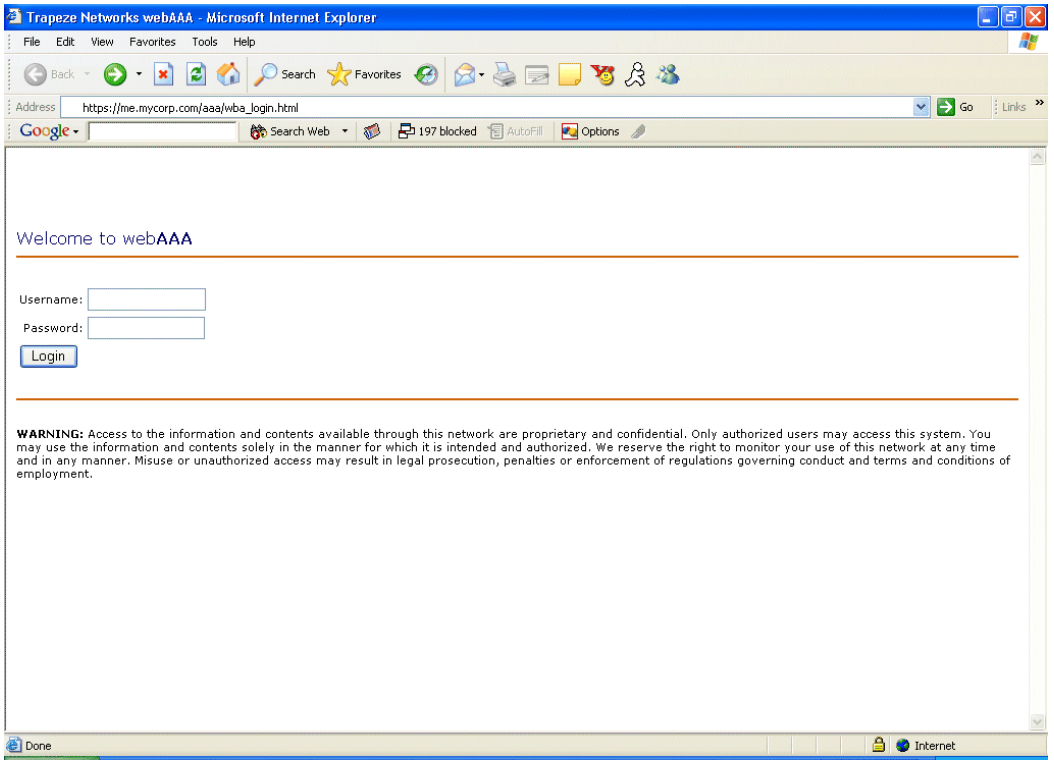
After authentication and authorization are complete, the **web-portal-mycorp** username is replaced with the username entered by the Web-based AAA user during login. The following example shows session information for the same user, but after the user is authorized to access resources on the network:

23x0# **show sessions network ssid mycorp**

```
User                             Sess  IP or MAC          VLAN            Port/
Name                               ID  Address            Name            Radio
------------------------------ ----  ------------------ --------------- -----
alice                             4* 192.168.12.101    corpvlan          3/1
bob                               5* 192.168.12.102    corpvlan          3/1
2 sessions total
```

Using a Custom Login Page

By default, WSS Software serves the Nortel login page for Web login.


Trapeze Networks webAAA - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://me.mycorp.com/aaa/wba_login.html
Go Links
Google Search Web 197 blocked AutoFill Options
Welcome to webAAA
Username:
Password:
Login
WARNING: Access to the information and contents available through this network are proprietary and confidential. Only authorized users may access this system. You may use the information and contents solely in the manner for which it is intended and authorized. We reserve the right to monitor your use of this network at any time and in any manner. Misuse or unauthorized access may result in legal prosecution, penalties or enforcement of regulations governing conduct and terms and conditions of employment.
Done
Internet

To serve a custom page instead, do the following:

1. Copy and modify the Nortel page, or create a new page.
2. Create a subdirectory in the user files area of the WSS switch's nonvolatile storage, and copy the custom page into the subdirectory.
3. Configure SSIDs and wired authentication ports to use the custom form, by specifying the location of the form.

Copying and Modifying the Nortel Login Page

To copy and modify the Nortel Web login page:

- Configure an unencrypted SSID on an WSS switch. The SSID is temporary does not need to be one you intend to use in your network. To configure the SSID, use the following commands:

  set service-profile *name* **ssid-name** *ssid-name* **ssid-type clear**

  set radio-profile *name* **service-profile** *name*

  set {**ap** *port-list* | **dap** *dap-num*} **radio** {**1** | **2**} **radio-profile** *name* **mode enable**

  Use the first two commands to configure a temporary SSID and temporary radio profile. Use the last command to map the temporary radio profile with the disabled radio, and enable the radio.

  Note. If the radio you plan to use is already in service, first you will need to disable the radio profile the radio is in and remove the radio from the profile.

- From your PC, attempt to directly access the temporary SSID. The WSS switch should serve the login page.
- Use your browser to save a copy of the page.
- Use a Web page editor or text editor to modify the page title, greeting, logo, and warning text.
- Save the modified page.

Custom Login Page Scenario

1. Do the following on the WSS switch:

   a. Create a temporary service profile and radio profile:

   23x0# **set radio-profile temprad service-profile tempsrvc**
   success: change accepted.

   b. Configure an unencrypted SSID on the service profile:

   23x0# **set service-profile ssid tempssid ssid-type clear**
   success: change accepted.

   c. Map a radio to the temporary radio profile and enable it:

   23x0# **set ap 2 radio 1 radio-profile temprad mode enable**
   success: change accepted.

2. From your PC, attempt to directly access the temporary SSID. The WSS switch serves the login page.
3. In the browser, select **File > Save As** to save the login page.
4. Edit the login page:

   a. Change the page title:

   ```
   <title>My Corp webAAA</title>
   ```

b Change the logo:

```
<img src="mycorp/mylogo.gif" width="143" height="65" border="0"
alt="Company Logo">
```

c Change the greeting:

```
<h3>Welcome to Mycorp's Wireless LAN</h3>
```

d Change the warning statement if desired:

```
<b>WARNING:</b>

My corp's warning text.
```

e ***Do not change the form (delimited by the <form name=> and </form> tags. The form values are required for the page to work properly.***

5 Save the modified page.

6 On the WSS switch, create a new subdirectory for the customized page. (The files must be on a TFTP server that the WSS switch can reach over the network.)

```
23x0# mkdir mycorp-webaaa
success: change accepted.
```

7 Copy the files for the customized page into the subdirectory:

```
23x0# copy tftp://10.1.1.1/mycorp-login.html mycorp-webaaa/mycorp-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]

23x0# copy tftp://10.1.1.1/mycorp-logo.jpg mycorp-webaaa/mycorp-logo.jpg
success: received 1202 bytes in 0.402 seconds [ 2112 bytes/sec]

23x0# dir mycorp-webaaa
================================================================================
file:
Filename                                    Size           Created
file:mycorp-login.html                      637 bytes   Aug 12 2004, 15:42:26
file:mycorp-logo.jpg                       1202 bytes   Aug 12 2004, 15:57:11
Total:        1839 bytes used, 206577 Kbytes free
```

8 Use the following command to configure the SSID to use the custom page:

set service-profile *name* **web-aaa-form** *url*

For the *url*, specify the full path; for example, *corpa-ssid/corpa.html*. If the custom login page includes gif or jpg images, their path names are interpreted relative to the directory from which the page is served.

9 Configure a Web-based AAA users and rules as described in "Configuring Portal Web-based AAA" on page 433.

Using Dynamic Fields in Web-based AAA Redirect URLs

You can include variables in the URL to which a Web-based AAA client is redirected after authentication and authorization. Table 30 lists the variables you can include in a redirect URL.

Table 30: Variables for Redirect URLs

Variable	Description
$u	Username of the Web AAA user
$v	VLAN to which the user was assigned during authorization
$s	SSID the user is on
$p	Name of the service profile that manages the parameters for the SSID

A URL string can also contain the literal characters $ and ?, if you use the values listed in Table 31.

Table 31: Values for Literal Characters

Variable	Description
$$	The literal character *$*
$q	The literal character *?*

You can configure a redirect URL for a group of users or for an individual user. For example, the following command configures a redirect URL containing a variable for the username:

```
23x0# set usergroup ancestors attr url http://myserver.com/$u.html
success: change accepted.
```

The variable applies to all Web-based AAA users in user group *ancestors*. When user *zinjanthropus* is successfully authenticated and authorized, WSS Software redirects the user to the following URL:

http://myserver.com/zinjanthropus.html

When user *piltdown* is successfully authenticated and authorized, WSS Software redirects the user to the following URL:

http://myserver.com/piltdown.html

The following example configures a redirect URL that contains a script argument using the literal character *?*:

```
23x0# set usergroup ancestors attr url https://saqqara.org/login.php$quser=$u
success: change accepted.
```

When user *djoser* is successfully authenticated and authorized, WSS Software redirects the user to the following URL:

https://saqqara.org/login.php?user=djoser

To verify configuration of a redirect URL and other user attributes, type the **show aaa** command.

Configuring Last-Resort Access

Users who are not authenticated and authorized by 802.1X methods or a MAC address can gain limited access to the network as guest users. You can optionally configure a special username called *last-resort-wired* (for wired authentication access) or *last-resort-**ssid***, where ***ssid*** is the SSID requested by the user. To match on the wildcard SSID name *any*, configure user *last-resort-any*, exactly as spelled here.

To configure a last-resort authentication rule, use the following command:

set authentication last-resort {**ssid** *ssid-name* | **wired**} *method1* [*method2*] [*method3*] [*method4*]

For example, to enable wireless users who request SSID *guestssid* to join the network on VLAN *k3*, type the following commands:

```
23x0# set authentication last-resort ssid guestssid local
success: change accepted
23x0# set user last-resort-guestssid attr vlan-name k3
success: change accepted
```

Note. Although WSS Software allows you to configure a user password for a last-resort user, the password has no effect. Last-resort users can never access an WSS in administrative mode and never require a password when authorized locally. However, if the last-resort user is authorized on a RADIUS server, the server might require a password. In this case, use the authorization password set on the WSS switch, which is *Nortel* by default.

Note. The fallthru authentication type must be set to **last-resort**. Otherwise, last-resort access is disabled. The default fallthru authentication type for wireless access to an SSID is **web**. The default for wired authentication access is **none**. (To change the fallthru authentication type for an SSID, see "Changing the Fallthru Authentication Type" on page 265. To change it for a wired authentication port, see "Setting a Port for a Wired Authentication User" on page 76.

Last-resort users configured on a RADIUS server require a password. Specify the authorization password (*Nortel* by default.) To change the password, see "Changing the MAC Authorization Password for RADIUS" on page 428. This procedure also applies for last-resort users.

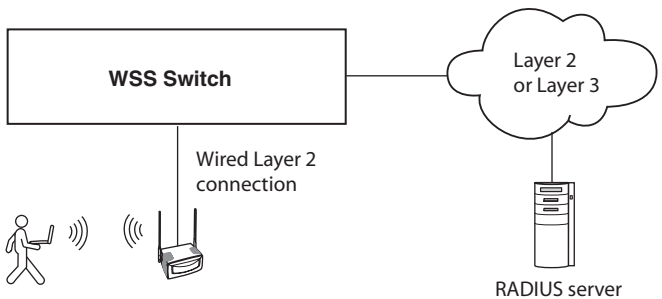
To ensure that your commands are configured, type the following command:

```
23x0# show aaa
...
set authentication last-resort ssid guestssid local
...
user last-resort-guestssid
   vlan-name = k3
```

Configuring AAA for Users of Third-Party APs

WSS Software Version 4.0 enables an WSS switch to provide network access for users associated with a third-party AP that has authenticated the users with RADIUS. You can connect a third-party AP to an WSS switch and configure the WSS to provide authorization for clients who authenticate and access the network through the AP. Figure 19 shows an example.

Figure 19: WSS Switch Serving as RADIUS Proxy



Authentication Process for 802.1X Users of a Third-Party AP

1. WSS Software uses MAC authentication to authenticate the AP.
2. The user contacts the AP and negotiates the authentication protocol to be used.
3. The AP, acting as a RADIUS client, sends a RADIUS request to the WSS.
4. The AP uses 802.1X to authenticate the user, using the WSS as its RADIUS server. The WSS proxies RADIUS requests from the AP to a real RADIUS server, depending on the authentication method specified in the proxy authentication rule for the user.
5. After successful RADIUS authentication of the user, WSS Software assigns authorization attributes to the user from the RADIUS server's access-accept response.

Requirements

Third-Party AP Requirements

- The third-party AP must be connected to the WSS switch through a wired Layer 2 link. WSS Software cannot provide data services if the AP and WSS are in different Layer 3 subnets.
- The AP must be configured as the WSS's RADIUS client.
- The AP must be configured so that all traffic for a given SSID is mapped to the same 802.1Q tagged VLAN. If the AP has multiple SSIDs, each SSID must use a different tag value.

WSS Switch Requirements

- The WSS port connected to the third-party AP must be configured as a wired authentication port. If SSID traffic from the AP is tagged, the same VLAN tag value must be used on the wired authentication port.
- A MAC authentication rule must be configured to authenticate the AP.
- The WSS must be configured as a RADIUS proxy for the AP. The WSS is a RADIUS server to the AP but remains a RADIUS client to the real RADIUS servers.
- An authentication proxy rule must be configured for the AP's users. The rule matches based on SSID and username, and selects the authentication method (a RADIUS server group) for proxying.

Configuring Authentication for 802.1X Users of a Third-Party AP

To configure WSS Software to authenticate 802.1X users of a third-party AP, use the commands below to do the following:

- Configure the port connected to the AP as a wired authentication port. Use the following command:

  set port type wired-auth *port-list* [**tag** *tag-list*] [**max-sessions** *num*] [**auth-fall-thru** {**last-resort** | **none** | **web-portal**}]

- Configure a MAC authentication rule for the AP. Use the following command:

  set authentication mac wired *mac-addr-wildcard method1*

- Configure the WSS port connected to the AP as a RADIUS proxy for the SSID supported by the AP. If SSID traffic from the AP is tagged, assign the same tag value to the WSS port. Use the following command:

  set radius proxy port *port-list* [**tag** *tag-value*] **ssid** *ssid-name*

- Add a RADIUS proxy entry for the AP. The proxy entry specifies the IP address of the AP and the UDP port on which the WSS switch listens for RADIUS traffic from the AP. Use the following command:

  set radius proxy client address *ip-address* [**port** *udp-port-number*] **key** *string*

- Configure a proxy authentication rule for the AP's users. Use the following command:

  set authentication proxy ssid *ssid-name user-wildcard radius-server-group*

For the *port-list* of the **set port type wired-auth** and **set radius proxy port** commands, specify the WSS port(s) connected to the third-party AP.

For the *ip-address* of the **set radius proxy client address** command, specify the IP address of the RADIUS client (the third-party AP). For the *udp-port-number*, specify the UDP port on which the WSS switch will listen for RADIUS traffic. The default is UDP port 1812.

The following command configures WSS ports 3 and 4 as wired authentication ports, and assigns tag value 104 to the ports:

```
23x0# set port type wired-auth 3-4 tag 104
success: change accepted.
```

You can specify multiple tag values. Specify the tag value for each SSID you plan to support.

The following command configures a MAC authentication rule that matches on the third-party AP's MAC address. Because the AP is connected to the WSS switch on a wired authentication port, the **wired** option is used.

```
23x0# set authentication mac wired aa:bb:cc:01:01:01 srvrgrp1
success: change accepted.
```

The following command maps SSID *mycorp* to packets received on port 3 or 4, using 802.1Q tag value 104:

```
23x0# set radius proxy port 3-4 tag 104 ssid mycorp
success: change accepted.
```

Enter a separate command for each SSID, and its tag value, you want the WSS to support.

The following command configures a RADIUS proxy entry for a third-party AP RADIUS client at 10.20.20.9, sending RADIUS traffic to the default UDP port 1812 on the WSS:

```
23x0# set radius proxy client address 10.20.20.9 key radkey1
success: change accepted.
```

The IP address is the AP's IP address. The key is the shared secret configured on the RADIUS servers. WSS Software uses the shared secret to authenticate and encrypt RADIUS communication.

The following command configures a proxy authentication rule that matches on all usernames associated with SSID *mycorp*. WSS Software uses RADIUS server group *srvrgrp1* to proxy RADIUS requests and hence to authenticate and authorize the users.

```
23x0# set authentication proxy ssid mycorp ** srvrgrp1
```

To verify the changes, use the **show config area aaa** command.

Assigning Authorization Attributes

Authorization attributes can be assigned to users in the local database or on remote servers. The attributes, which include access control list (ACL) filters, VLAN membership, encryption type, session time-out period, and other session characteristics, let you control how and when users access the network. When a user or group is authenticated, the local database or RADIUS server passes the authorization attributes to WSS Software to characterize the user's session.

The VLAN attribute is required. WSS Software can authorize a user to access the network only if the VLAN to place the user on is specified.

Table 32 on page 446 lists the authorization attributes supported by WSS Software. (For brief descriptions of all the RADIUS attributes and Nortel vendor-specific attributes supported by WSS Software, as well as the vendor ID and types for Nortel VSAs configured on a RADIUS server, see "Supported RADIUS Attributes," on page 599.)

Table 32: Authentication Attributes for Local Users

Attribute	Description	Valid Values
encryption-type	Type of encryption required for access by the client. Clients who attempt to use an unauthorized encryption method are rejected.	One of the following numbers that identifies an encryption algorithm: • **1**—AES_CCM (Advanced Encryption Standard using Counter with CBC-MAC) • **2**—Reserved • **4**—TKIP (Temporal Key Integrity Protocol) • **8**—WEP_104 (the default) (Wired-Equivalent Privacy protocol using 104 bits of key strength) • **16**—WEP_40 (Wired-Equivalent Privacy protocol using 40 bits of key strength) • **32**—NONE (no encryption) • **64**—Static WEP In addition to these values, you can specify a sum of them for a combination of allowed encryption types. For example, to specify WEP_104 and WEP_40, use **24**.
end-date	Date and time after which the user is no longer allowed to be on the network.	Date and time, in the following format: YY/MM/DD-HH:MM You can use **end-date** alone or with **start-date**. You also can use **start-date**, **end-date**, or both in conjunction with **time-of-day**.

Table 32: Authentication Attributes for Local Users (continued)

Attribute	Description	Valid Values
filter-id (network access mode only)	Security access control list (ACL), to permit or deny traffic received (input) or sent (output) by the WSS switch. (For more information about security ACLs, see "Configuring and Managing Security ACLs," on page 351.)	Name of an existing security ACL, up to 253 alphanumeric characters, with no tabs or spaces. • Use *acl-name***.in** to filter traffic that enters the switch *from users* through an AP access point or wired authentication port, or from the network through a network port. • Use *acl-name***.out** to filter traffic sent from the switch *to users* through an AP access point or wired authentication port, or from the network through a network port. **Note:** If the Filter-Id value returned through the authentication and authorization process does not match the name of a committed security ACL in the WSS, the user fails authorization and is unable to authenticate.
idle-timeout	This option is not implemented in the current WSS Software version.	
mobility-profile (network access mode only)	Mobility Profile attribute for the user. (For more information, see "Configuring a Mobility Profile" on page 468.)	Name of an existing Mobility Profile, which can be up to 32 alphanumeric characters, with no tabs or spaces. **Note:** If the Mobility Profile feature is enabled, and a user is assigned the name of a Mobility Profile that does not exist on the WSS switch, the user is denied access.
service-type	Type of access the user is requesting.	One of the following numbers: • **2**—Framed; for network user access • **6**—Administrative; for administrative access to the WSS switch, with authorization to access the enabled (configuration) mode. The user must enter the **enable** command and the correct enable password to access the enabled mode. • **7**—NAS-Prompt; for administrative access to the nonenabled mode only. In this mode, the user can still enter the **enable** command and the correct enable password to access the enabled mode. For administrative sessions, the WSS switch always sends 6 (Administrative). The RADIUS server can reply with one of the values listed above. If the service-type is not set on the RADIUS server, administrative users receive NAS-Prompt access, and network users receive Framed access.
session-timeout (network access mode only)	Maximum number of seconds for the user's session.	Number between 0 and 4,294,967,296 seconds (approximately 136.2 years).

Table 32: Authentication Attributes for Local Users (continued)

Attribute	Description	Valid Values
ssid (network access mode only)	SSID the user is allowed to access after authentication.	Name of the SSID you want the user to use. The SSID must be configured in a service profile, and the service profile must be used by a radio profile assigned to Nortel radios in the Mobility Domain.
start-date	Date and time at which the user becomes eligible to access the network. WSS Software does not authenticate the user unless the attempt to access the network occurs at or after the specified date and time, but before the end-date (if specified).	Date and time, in the following format: YY/MM/DD-HH:MM You can use **start-date** alone or with **end-date**. You also can use **start-date**, **end-date**, or both in conjunction with **time-of-day**.
time-of-day (network access mode only)	Day(s) and time(s) during which the user is permitted to log into the network. After authorization, the user's session can last until either the Time-Of-Day range or the Session-Timeout duration (if set) expires, whichever is shorter.	One of the following: • **never**—Access is always denied. • **any**—Access is always allowed. • **al**—Access is always allowed. • One or more ranges of values that consist of one of the following day designations (required), and a time range in *hhmm-hhmm* 4-digit 24-hour format (optional): • **mo**—Monday • **tu**—Tuesday • **we**—Wednesday • **th**—Thursday • **fr**—Friday • **sa**—Saturday • **su**—Sunday • **wk**—Any day between Monday and Friday Separate values or a series of ranges (except time ranges) with commas (,) or a vertical bar (|). Do not use spaces. The maximum number of characters is 253. **Note:** You can use **time-of-day** in conjunction with **start-date**, **end-date**, or both.

Table 32: Authentication Attributes for Local Users (continued)

Attribute	Description	Valid Values
url (network access mode only)	URL to which the user is redirected after successful Web-based AAA.	Web URL, in standard format. For example: http://www.example.com **Note:** You must include the *http://* portion. You can dynamically include any of the variables in the URL string: • **$u**—Username • **$v**—VLAN • **$s**—SSID • **$p**—Service profile name To use the literal character $ or ?, use the following: • **$$** • **$q**
vlan-name (network access mode only)	Virtual LAN (VLAN) assignment. **Note:** On some RADIUS servers, you might need to use the standard RADIUS attribute Tunnel-Pvt-Group-ID, instead of VLAN-Name.	Name of a VLAN that you want the user to use. The VLAN must be configured on an WSS switch within the Mobility Domain to which this WSS switch belongs.

Assigning Attributes to Users and Groups

You can assign authorization attributes to individual users or groups of users. Use any of the following commands to assign an attribute to a user or group in the local WSS database and specify its value:

set user *username* **attr** *attribute-name value*

set usergroup *group-name* **attr** *attribute-name value*

set mac-user *mac-addr* **attr** *attribute-name value*

set mac-usergroup *group-name* **attr** *attribute-name value*

To change the value of an authorization attribute, reenter the command with the new value.

To assign an authorization attribute to a user's configuration on a RADIUS server, see the documentation for your RADIUS server.

Assigning a Security ACL to a User or a Group

Once a security access control list (ACL) is defined and committed, it can be applied dynamically and automatically to users and user groups through the 802.1X authentication and authorization process. When you assign a Filter-Id attribute to a user or group, the security ACL name value is entered as an authorization attribute into the user or group record in the local WSS database or RADIUS server.



Note. If the Filter-Id value returned through the authentication and authorization process does not match the name of a committed security ACL in the WSS, the user fails authorization and cannot be connected.

(For details about security ACLs, see "Configuring and Managing Security ACLs," on page 351.)

Assigning a Security ACL Locally

To use the local WSS database to restrict a user, a MAC user, or a group of users or MAC users to the permissions stored within a committed security ACL, use the following commands:

Security ACL Target	Commands
User authenticated by a password	**set user** *username* **attr filter-id** *acl-name***.in** **set user** *username* **attr filter-id** *acl-name***.out**
Group of users authenticated by a password	**set usergroup** *groupname* **attr filter-id** *acl-name***.in** **set usergroup** *groupname* **attr filter-id** *acl-name***.out**
User authenticated by a MAC address	**set mac-user** *username* **attr filter-id** *acl-name***.in** **set mac-user** *username* **attr filter-id** *acl-name***.out**
Group of users authenticated by a MAC address	**set mac-usergroup** *groupname* **attr filter-id** *acl-name***.in** **set mac-usergroup** *groupname* **attr filter-id** *acl-name***.out**

You can set filters for incoming and outgoing packets:

- Use *acl-name***.in** to filter traffic that enters the WSS switch *from users* through an AP access point or wired authentication port, or from the network through a network port.
- Use *acl-name***.out** to filter traffic sent from the WSS switch *to users* through an AP access point or wired authentication port, or from the network through a network port.

For example, the following command applies security ACL *acl-101* to packets coming into the WSS from user *Jose*:

```
23x0# set user Jose attr filter-id acl-101.in
success: change accepted.
```

The following command applies the incoming filters of *acl-101* to the users who belong to the group *eastcoasters*:

```
23x0# set usergroup eastcoasters attr filter-id acl-101.in
```

```
success: change accepted.
```

Assigning a Security ACL on a RADIUS Server

To assign a security ACL name as the Filter-Id authorization attribute of a user or group record on a RADIUS server, see the documentation for your RADIUS server.

Clearing a Security ACL from a User or Group

To clear a security ACL from the profile of a user, MAC user, or group of users or MAC users in the local WSS database, use the following commands:

clear user *username* **attr filter-id**

clear usergroup *groupname* **attr filter-id**

clear mac-user *username* **attr filter-id**

`clear` **mac-**`usergroup` *`groupname`* `attr filter-id`

If you have assigned both an incoming and an outgoing filter to a user or group, enter the appropriate command twice to delete both security ACLs. Verify the deletions by entering the **show aaa** command and checking the output.

To delete a security ACL from a user's configuration on a RADIUS server, see the documentation for your RADIUS server.

Assigning Encryption Types to Wireless Users

When a user turns on a wireless laptop or PDA, the device attempts to find an access point and form an association with it. Because AP access ports support the encryption of wireless traffic, clients can choose an encryption type to use. You can configure AP access ports to use the encryption algorithms supported by the Wi-Fi Protected Access (WPA) security enhancement to the IEEE 802.11 wireless standard. (For details, see "Configuring User Encryption," on page 191.)

If you have configured AP access ports to use specific encryption algorithms, you can enforce the type of encryption a user or group must have to access the network. When you assign the Encryption-Type attribute to a user or group, the encryption type or types are entered as an authorization attribute into the user or group record in the local WSS database or on the RADIUS server. Encryption-Type is a Nortel vendor-specific attribute (VSA).

Clients who attempt to use an unauthorized encryption method are rejected.

Assigning and Clearing Encryption Types Locally

To restrict wireless uses or groups with user profiles in the local WSS database to particular encryption algorithms for accessing the network, use one of the following commands:

set user *username* **attr encryption-type** *value*

set usergroup *groupname* **attr encryption-type** *value*

set mac-user *username* **attr encryption-type** *value*

set mac-usergroup *groupname* **attr encryption-type** *value*

WSS Software supports the following values for Encryption-Type, listed from most secure to least secure. (For user encryption details, see "Configuring User Encryption," on page 191.)

Encryption-Type Value	Encryption Algorithm Assigned
1	Advanced Encryption Standard using Counter with Cipher Block Chaining Message Authentication Code (CBC-MAC)—or AES_CCM.
2	Reserved.
4	Temporal Key Integrity Protocol (TKIP).
8	Wired-Equivalent Privacy protocol using 104 bits of key strength (WEP_104). This is the default.
16	Wired-Equivalent Privacy protocol using 40 bits of key strength (WEP_40).
32	No encryption.
64	Static WEP

For example, the following command restricts the MAC user group *mac-fans* to access the network by using only TKIP:

```
23x0# set mac-usergroup mac-fans attr encryption-type 4
success: change accepted.
```

You can also specify a combination of allowed encryption types by summing the values. For example, the following command allows *mac-fans* to associate using either TKIP or WEP_104:

```
23x0# set mac-usergroup mac-fans attr encryption-type 12
success: change accepted.
```

To clear an encryption type from the profile of a use or group of users in the local WSS database, use one of the following commands:

clear user *username* **attr encryption-type**

clear usergroup *groupname* **attr encryption-type**

clear mac-user *username* **attr encryption-type**

clear mac-usergroup *groupname* **attr encryption-type**

Assigning and Clearing Encryption Types on a RADIUS Server

To assign or delete an encryption algorithm as the Encryption-Type authorization attribute in a user or group record on a RADIUS server, see the documentation for your RADIUS server.

Overriding or Adding Attributes Locally with a Location Policy

During the login process, the AAA authorization process is started immediately after clients are authenticated to use the WSS switch. During authorization, WSS Software assigns the user to a VLAN and applies optional user attributes, such as a session timeout value and one or more security ACL filters.

A *location policy* is a set of rules that enables you to locally set or change authorization attributes for a user after the user is authorized by AAA, without making changes to the AAA server. For example, you might want to enforce VLAN membership and security ACL policies on a particular WSS based on a client's organization or physical location, or assign a VLAN to users who have no AAA assignment. For these situations, you can configure the location policy on the switch.

You can use a location policy to locally set or change the Filter-Id and VLAN-Name authorization attributes obtained from AAA.

About the Location Policy

Each WSS switch can have one location policy. The location policy consists of a set of rules. Each rule contains conditions, and an action to perform if all conditions in the rule match.

The action can be one of the following:

- Deny access to the network
- Permit access, but set or change the user's VLAN assignment, inbound ACL, outbound ACL, or any combination of these attributes

The conditions can be one or more of the following:

- AAA-assigned VLAN
- Username
- AP access port, Distributed AP number, or wired authentication port through which the user accessed the network
- SSID name with which the user is associated

Conditions within a rule are ANDed. All conditions in the rule must match in order for WSS Software to take the specified action. If the location policy contains multiple rules, WSS Software compares the user information to the rules one at a time, in the order the rules appear in the switch's configuration file, beginning with the rule at the top of the list. WSS Software continues comparing until a user matches all conditions in a rule or until there are no more rules.

Any authorization attributes not changed by the location policy remain active.

How the Location Policy Differs from a Security ACL

Although structurally similar, the location policy and security ACLs have different functions. The location policy on an WSS switch can be used to locally redirect a user to a different VLAN or locally control the traffic to and from a user.

In contrast, security ACLs are packet filters applied to the user throughout a Mobility Domain. (For more information, see "Configuring and Managing Security ACLs," on page 351.)

You can use the location policy to locally apply a security ACL to a user.

Setting the Location Policy

To enable the location policy function on an WSS switch, you must create at least one location policy rule with one of the following commands:

set location policy deny if {**ssid** *operator ssid-name* | **vlan** *operator vlan-wildcard* | **user** *operator user-wildcard* | **port** *port-list* | **dap** *dap-num*}
[**before** *rule-number* | **modify** *rule-number*]

set location policy permit {**vlan** *vlan-name* | **inacl** *inacl-name* | **outacl** *outacl-name*} **if** {**ssid** *operator ssid-name* | **vlan** *operator vlan-wildcard* | **user** *operator user-wildcard* | **port** *port-list* | **dap** *dap-num*}
[**before** *rule-number* | **modify** *rule-number*]

Note. Asterisks (wildcards) are not supported in SSID names. You must specify the complete SSID name.

You must specify whether to permit or deny access, and you must identify a VLAN, username, or access point to match. Use one of the following operators to specify how the rule must match the VLAN or username:

- **eq**—Applies the location policy rule to all users assigned VLAN names matching *vlan-wildcard* or having usernames that match *user-wildcard*.

  (Like a user wildcard, a VLAN wildcard is a way to group VLANs for use in this command. For more information, see "VLAN Wildcards" on page 40.)

- **neq**—Applies the location policy rule to all users assigned VLAN names *not* matching *vlan-wildcard* or having usernames that *do not* match *user-wildcard*.

For example, the following command denies network access to all users matching *.theirfirm.com, causing them to fail authorization:

```
23x0# set location policy deny if user eq *.theirfirm.com
```

The following command authorizes access to the *guest_1* VLAN for all users who do not match *.ourfirm.com:

```
23x0# set location policy permit vlan guest_1 if user neq *.ourfirm.com
```

The following command places all users who are authorized for SSID *tempvendor_a* into VLAN *kiosk_1*:

```
23x0# set location policy permit vlan kiosk_1 if ssid eq tempvendor_a
success: change accepted.
```

Applying Security ACLs in a Location Policy Rule

When reassigning security ACL filters, specify whether the filter is an input filter or an output filter, as follows:

- Input filter—Use **inacl** *inacl-name* to filter traffic that *enters* the switch from users through an AP access point or wired authentication port, or from the network through a network port.
- Output filter—Use **outacl** *outacl-name* to filter traffic sent *from* the switch to users through an AP access point or wired authentication port, or from the network through a network port.

For example, the following command authorizes users at *.ny.ourfirm.com to access the *bld4.tac* VLAN, and applies the security ACL *tac_24* to the traffic they receive:

```
23x0# set location policy permit vlan bld4.tac outacl tac_24 if user eq *.ny.ourfirm.com
```

The following command authorizes access to users on VLANs with names matching *bld4.** and applies security ACLs *svcs_2* to the traffic they send and *svcs_3* to the traffic they receive:

23x0# **set location policy permit inacl svcs_2 outacl svcs_3 if vlan eq bldg4.***

You can optionally add the suffixes **.in** and **.out** to *inacl-name* and *outacl-name* for consistency with their usage in entries stored in the local WSS database.

Displaying and Positioning Location Policy Rules

The order of location policy rules is significant. WSS Software checks a location policy rule that is higher in the list before those lower in the list. Rules are listed in the order in which you create them, unless you move them.

To position location policy rules within the location policy, use **before** *rule-number* and **modify** *rule-number* in the **set location policy** command, or use the **clear location policy** *rule-number* command.

For example, suppose you have configured the following location policy rules:

```
WSS-20 show location policy
Id Clauses
-----------------------------------------------------------------
1) deny if user eq *.theirfirm.com
2) permit vlan guest_1 if vlan neq *.ourfirm.com
3) permit vlan bld4.tac inacl tac_24.in if user eq *.ny.ourfirm.com
4) permit inacl svcs_2.in outacl svcs_3.out if vlan eq bldg4.*
```

To move the first rule to the end of the list and display the results, type the following commands:

```
WSS-20 clear location policy 1
success: clause 1 is removed.

WSS-20 set location policy deny if user eq *.theirfirm.com

WSS-20 show location policy
Id Clauses
-----------------------------------------------------------------
1) permit vlan guest_1 if vlan neq *.ourfirm.com
2) permit vlan bld4.tac inacl tac_24.in if user eq *.ny.ourfirm.com
3) permit inacl svcs_2.in outacl svcs_3.out if vlan eq bldg4.*
4) deny if user eq *.theirfirm.com
```

Clearing Location Policy Rules and Disabling the Location Policy

To delete a location policy rule, use the following command:

clear location policy *rule-number*

Type **show location policy** to display the numbers of configured location policy rules. To disable the location policy on an WSS switch, delete all the location policy rules.

Configuring Accounting for Wireless Network Users

Accounting records come in three types: start-stop, stop-only, and update for network users. The records provide information about network resource usage.

To set accounting, type the following command:

set accounting {admin | console | dot1x | mac | web}
{ssid *ssid-name* **| wired} {***user-wildcard* **|** *mac-addr-wildcard***}**
{start-stop | stop-only} *method1* **[***method2***] [***method3***] [***method4***]**

For example, to store start-stop accounting records at example.com for 802.1X users of SSID *mycorp* in the local database, type the following command:

```
23x0# set accounting dot1x ssid mycorp *@example.com start-stop local
success: change accepted.
```

The accounting records can contain the following session information:

Start Records	Update and Stop Records
Session date and time	Session date and time
Location of authentication (if any): RADIUS server (1) or local database (2)	Location of authentication (if any): RADIUS server (1) or local database (2)
ID for related sessions	ID for related sessions
Username	Username
Session duration	Session duration
Timestamp	Timestamp
VLAN name	VLAN name
Client’s MAC address	Client’s MAC address
AP port number and radio number	AP port number and radio number
AP access port’s MAC address	AP access port’s MAC address
	Number of octets received by the WSS switch
	Number of octets sent by the switch
	Number of packets received by the switch
	Number of packets sent by the switch

(For details about **show accounting statistics** output, see the *Nortel Mobility System Software Command Reference*. For information about accounting update records, see "Viewing Roaming Accounting Records" on page 463. To configure accounting on a RADIUS server, see the documentation for your RADIUS server.)

Viewing Local Accounting Records

To view local accounting records, type the following command:

```
23x0# show accounting statistics
Sep2611:01:48Acct-Status-Type=STARTAcct-Authentic=2User-Name=geetha
AAA_TTY_ATTR=2 Event-Timestamp=1064599308
Sept2612:50:21Acct-Status-Type=STOPAcct-Authentic=2User-Name=geetha
AAA_TTY_ATTR=2 Acct-Session-Time=6513 Event-Timestamp=1064605821
Acct-Output-Octets=332 Acct-Input-Octets=61
Sep2612:50:33Acct-Status-Type=STARTAcct-Authentic=2User-Name=geetha
AAA_TTY_ATTR=2 Event-Timestamp=1064605833
```

For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.

Viewing Roaming Accounting Records

During roaming, accounting is treated as a continuation of an existing session, rather than a new session. The following sample output shows a wireless user roaming from one WSS switch to another WSS switch.

From the accounting records, you can determine the user's activities by viewing the Acct-Status-Type, which varies from START to UPDATE to STOP, and the Called-Station-Id, which is the MAC address of the AP access point through which the wireless user accessed the network. The Acct-Multi-Session-Id is guaranteed to be globally unique for the client.

By entering **show accounting statistics** commands on each WSS switch involved in the roaming, you can determine the user's movements between WSS switches when accounting is configured locally.

The user started on WSS-20-0013:

```
WSS-20-0013# show accounting statistics
May 21 17:01:32
Acct-Status-Type=START
Acct-Authentic=2
User-Name=Administrator@example.com
Acct-Multi-Session-Id=SESSION-4-1106424789
Event-Timestamp=1053536492
Vlan-Name=default
Calling-Station-Id=00-06-25-09-39-5D
Nas-Port-Id=1/1
Called-Station-Id=00-0B-0E-76-56-A8
```

The user roamed to WSS-20-0017.

```
WSS-20-0017# show accounting statistics
May 21 17:05:00
Acct-Status-Type=UPDATE
Acct-Authentic=2
Acct-Multi-Session-Id=SESSION-4-1106424789
User-Name=Administrator@example.com
Acct-Session-Time=209
Acct-Output-Octets=1280
Acct-Input-Octets=1920
Acct-Output-Packets=10
Acct-Input-Packets=15
Event-Timestamp=1053536700
Vlan-Name=default
Calling-Station-Id=00-06-25-09-39-5D
Nas-Port-Id=2/1
Called-Station-Id=00-0B-0E-76-56-A0
```

The user terminated the session on WSS-20-0017:

```
WSS-20-0017# show accounting statistics
May 21 17:07:32
Acct-Status-Type=STOP
Acct-Authentic=2
```

```
Acct-Multi-Session-Id=SESSION-4-1106424789
User-Name=Administrator@example.com
Acct-Session-Time=361
Event-Timestamp=1053536852
Acct-Output-Octets=2560
Acct-Input-Octets=5760
Acct-Output-Packets=20
Acct-Input-Packets=45
Vlan-Name=default
Calling-Station-Id=00-06-25-09-39-5D
Nas-Port-Id=2/1
Called-Station-Id=00-0B-0E-76-56-A0
```

If you configured accounting records to be sent to a RADIUS server, you can view the records of user roaming at the RADIUS server. (For more information on these attributes, see "Supported RADIUS Attributes," on page 599.)

For information about requesting accounting records from the RADIUS server, see the documentation for your RADIUS server.

Displaying the AAA Configuration

To view the results of the AAA commands you have set and verify their order, type the **show aaa** command. The order in which the commands appear in the output determines the order in which WSS Software matches them to users.

(Sometimes the order might not be what you intended. See "Avoiding AAA Problems in Configuration Order" on page 465.)

For example:

```
23x0# show aaa
Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=0 key=(null) author-pass=(null)

Radius Servers
Server                    Addr            Ports    T/o Tries Dead State
-------------------------------------------------------------------------
rs-3                   198.162.1.1      1821 1813   5     3     0     UP
rs-4                   198.168.1.2      1821 1813   77    11    2     UP
rs-5                   198.162.1.3      1821 1813   42    23    0     UP

Server groups
   sg1: rs-3
   sg2: rs-4
   sg3: rs-5
set authentication admin Jose sg3
```

```
set authentication console * none
set authentication mac ssid mycorp * local
set authentication dot1x ssid mycorp Geetha eap-tls
set authentication dot1x ssid mycorp * peap-mschapv2 sg1 sg2 sg3
set accounting dot1x Nin ssid mycorp stop-only sg2
set accounting admin Natasha start-stop local
set authentication last-resort ssid guestssid local


user Nin
   Password = 082c6c64060b (encrypted)
   Filter-Id = acl-999.in
   Filter-Id = acl-999.out

user last-resort-guestssid
   Vlan-Name = k2

mac-user 01:02:03:04:05:06

usergroup eastcoasters

   session-timeout = 99
```

For information about the fields in the output, see the *Nortel Mobility System Software Command Reference.*

Avoiding AAA Problems in Configuration Order

Using the Wildcard "Any" as the SSID Name in Authentication Rules

You can configure an authentication rule to match on all SSID strings by using the SSID string *any* in the rule. For example, the following rule matches on all SSID strings requested by all users:

set authentication web ssid any ** sg1

WSS Software checks authentication rules in the order they appear in the configuration file. As a result, if a rule with SSID **any** appears in the configuration before a rule that matches on a specific SSID for the same authentication type and userwildcard, the rule with **any** always matches first.

To ensure the authentication behavior that you expect, place the most specific rules first and place rules with SSID **any** last. For example, to ensure that users who request SSID *corpa* are authenticated using RADIUS server group *corpasrvr*, place the following rule in the configuration before the rule with SSID **any**:

set authentication web ssid corpa ** corpasrvr

Here is an example of a AAA configuration where the most-specific rules for 802.1Xare first and the rules with **any** are last:

```
23x0# show aaa
...
```

```
set authentication dot1x ssid mycorp Geetha eap-tls
set authentication dot1x ssid mycorp * peap-mschapv2 sg1 sg2 sg3
set authentication dot1x ssid any ** peap-mschapv2 sg1 sg2 sg3
```

Using Authentication and Accounting Rules Together

When you use accounting commands with authentication commands and identify users with user wildcards, WSS Software might not process the commands in the order you entered them. As a result, user authentication or accounting might not proceed as you intend, or valid users might fail authentication and be shut out of the network.

You can prevent these problems by using duplicate user wildcards for authentication and accounting and entering the commands in pairs.

Configuration Producing an Incorrect Processing Order

For example, suppose you initially set up start-stop accounting as follows for all 802.1X users through RADIUS server group 1:

```
23x0# set accounting dot1x ssid mycorp * start-stop group1
success: change accepted.
```

You then set up PEAP-MS-CHAP-V2 authentication and authorization for all users at EXAMPLE/ at server group 1. Finally, you set up PEAP-MS-CHAP-V2 authentication and authorization for all users in the local WSS database, with the intention that EXAMPLE users are to be processed first:

```
23x0# set authentication dot1x ssid mycorp EXAMPLE/* peap-mschapv2 group1
success: change accepted.
```

```
23x0# set authentication dot1x ssid mycorp * peap-mschapv2 local
success: change accepted.
```

The following configuration order results. The authentication commands are reversed, and WSS Software processes the authentication of all 802.1X users in the local database and ignores the command for EXAMPLE/ users.

```
23x0# show aaa
...
set accounting dot1x ssid mycorp * start-stop group1
set authentication dot1x ssid mycorp * peap-mschapv2 local
set authentication dot1x ssid mycorp EXAMPLE/* peap-mschapv2 group1
```

Configuration for a Correct Processing Order

To avoid processing errors for authentication and accounting commands that include order-sensitive user wildcards, enter the commands for each user wildcard in pairs.

For example, to set accounting and authorization for 802.1X users as you intended in "Configuration Producing an Incorrect Processing Order" on page 467, enter an accounting and authentication command for each user wildcard in the order in which you want them processed:

```
23x0# set accounting dot1x ssid mycorp EXAMPLE/* start-stop group1
success: change accepted.
```

```
23x0# set authentication dot1x ssid mycorp EXAMPLE/* peap-mschapv2 group1
success: change accepted.
```

```
23x0# set accounting dot1x ssid mycorp * start-stop group1
```

```
success: change accepted.
```

```
23x0# set authentication dot1x ssid mycorp * peap-mschapv2 local
success: change accepted.
```

The configuration order now shows that all 802.1X users are processed as you intended:

```
23x0# show aaa
...
set accounting dot1x ssid mycorp EXAMPLE/* start-stop group1
set authentication dot1x ssid mycorp EXAMPLE/* peap-mschapv2 group1
set accounting dot1x ssid mycorp * start-stop group1
set authentication dot1x ssid mycorp * peap-mschapv2 local
```

Configuring a Mobility Profile

A Mobility Profile is a way of specifying, on a per-user basis, those users who are allowed access to specified AP access ports and wired authentication ports on an WSS switch. In this way, you can constrain the areas to which a user can roam. You first create a Mobility Profile, assign it to one or more users, and finally enable the Mobility Profile feature on the WSS.



Caution! When Mobility Profile attributes are enabled, a user is denied access if assigned a Mobility-Profile attribute in the local WSS switch database or RADIUS server and no Mobility Profile of that name exists on the WSS switch.

Use the following command to create a Mobility Profile by giving it a name and identifying the accessible port or ports:

set mobility-profile name *name*
{port {none | **all** | *port-list***}** | **{dap {none** | **all** | *dap-num***}}**

Specifying **none** prevents users assigned to the Mobility Profile from accessing any AP access ports, Distributed APs, or wired authentication ports on the WSS. Specifying **all** allows the users access to all of the ports or Distributed APs.

Specifying an individual port or Distributed AP number or a list limits access to those ports or APs. For example, the following command creates a Mobility Profile named *roses-profile* that allows access through ports 2 through 4, port 7, and port 9:

```
23x0# set mobility-profile name roses-profile port 2-4,7,9
success: change accepted.
```

You can then assign this Mobility Profile to one or more users. For example, to assign the Mobility Profile *roses-profile* to all users at EXAMPLE\, type the following command:

```
23x0# set user EXAMPLE\* attr mobility-profile roses-profile
success: change accepted.
```

(For a list of the commands for assigning attributes, see "Assigning Attributes to Users and Groups" on page 450.)

During 802.1X authorization for clients at EXAMPLE\, WSS Software must search for the Mobility Profile named *roses-profile*. If it is not found, the authorization fails and clients with usernames like EXAMPLE\jose and EXAMPLE\tamara are rejected.

If *roses-profile* is configured for EXAMPLE\ users on your WSS, WSS Software checks its port list. If, for example, the current port for EXAMPLE\jose's connection is on the list of allowed ports specified in *roses-profile*, the connection is allowed to proceed. If the port is not in the list (for example, EXAMPLE\jose is on port 12, which is not in the port list), the authorization fails and client EXAMPLE\jose is rejected.

The Mobility Profile feature is disabled by default. You must enable Mobility Profile attributes on the WSS switch to use it. You can enable or disable the feature for the whole WSS only. If the Mobility Profile feature is disabled, all Mobility Profile attributes are ignored.

To put Mobility Profile attributes into effect on an WSS, type the following command:

```
23x0# set mobility-profile mode enable
success: change accepted.
```

To display the name of each Mobility Profile and its ports, type the following command:

```
23x0# show mobility-profile
Mobility Profiles
Name                    Ports
========================
roses-profile
                    AP 2
                    AP 3
                    AP 4
                    AP 7
                    AP 9
```

To remove a Mobility Profile, type the following command:

clear mobility-profile *name*

Network User Configuration Scenarios

The following scenarios provide examples of ways in which you use AAA commands to configure access for users:

- "General Use of Network User Commands" on page 470
- "Enabling RADIUS Pass-Through Authentication" on page 472
- "Enabling PEAP-MS-CHAP-V2 Authentication" on page 473
- "Enabling PEAP-MS-CHAP-V2 Offload" on page 474
- "Combining 802.1X Acceleration with Pass-Through Authentication" on page 475
- "Overriding AAA-Assigned VLANs" on page 476

General Use of Network User Commands

The following example illustrates how to configure IEEE 802.1X network users for authentication, accounting, ACL filtering, and Mobility Profile assignment:

1. Configure all 802.1X users of SSID *mycorp* at EXAMPLE to be authenticated by server group *shorebirds.* Type the following command:

   ```
   2370# set authentication dot1x ssid mycorp EXAMPLE\* pass-through shorebirds
   ```

2. Configure stop-only accounting for all *mycorp* users at EXAMPLE, for accounting records to be stored locally. Type the following command:

   ```
   23x0# set accounting dot1x ssid mycorp EXAMPLE\* stop-only local
   success: change accepted.
   ```

3. Configure an ACL to filter the inbound packets for each user at EXAMPLE. Type the following command for *each* user:

   ```
   23x0# set user EXAMPLE\username attr filter-id acl-101.in
   ```

   This command applies the access list named *acl-101* to each user at EXAMPLE.

4. To display the ACL, type the following command:

   ```
   23x0# show security acl info acl-101
   set security acl ip acl-101 (hits #0 0)
   ---------------------------------------------------
    1. permit IP source IP 192.168.1.1 0.0.0.255 destination IP any
   enable-hits
   ```

   (For more information about ACLs, see "Configuring and Managing Security ACLs," on page 351.)

5. Create a Mobility Profile called *tulip* by typing the following commands:

   ```
   23x0# set mobility-profile name tulip port 2,5-9
   success: change accepted.

   23x0# set mobility-profile mode enable
   success: change accepted.

   23x0# show mobility-profile
   Mobility Profiles
   Name                  Ports
   ========================
   tulip
                     AP 2
                     AP 6
                     AP 7
                     AP 8
                     AP 9
   ```

6. To assign Mobility Profile *tulip* to all users at EXAMPLE, type the following command for *each* EXAMPLE\ user:

   ```
   23x0# set user EXAMPLE\username attr mobility-profile tulip
   ```

Users at EXAMPLE are now restricted to ports 2 and 5 through 9, as specified in the *tulip* Mobility Profile configuration.

7 Use the **show aaa** command to verify your configuration. Type the following command:

```
23x0# show aaa
Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=0 key=(null) author-pass=(null)

Radius Servers
Server                  Addr           Ports   T/o Tries Dead
State
-------------------------------------------------------------
----

set accounting dot1x ssid mycorp EXAMPLE\* stop-only local
set authentication dot1x ssid mycorp EXAMPLE\* pass-through
shorebirds

user tech
   Password = 1315021018 (encrypted)

user EXAMPLE/nin
   filter-id = acl.101.in
   mobility-profile = tulip

user EXAMPLE/tamara
   filter-id = acl.101.in
   mobility-profile = tulip
...
```

8 Save the configuration:

```
WSS-20 save config
success: configuration saved.
```

Enabling RADIUS Pass-Through Authentication

The following example illustrates how to enable RADIUS pass-through authentication for all 802.1X network users:

1. Configure the RADIUS server *r1* at IP address 10.1.1.1 with the string *sunny* for the key. Type the following command:

   23x0# **set radius server r1 address 10.1.1.1 key sunny**

2. Configure the server group *sg1* with member *r1*. Type the following command:

   23x0# **set server group sg1 members r1**

3. Enable all 802.1X users of SSID *mycorp* to authenticate through pass-through to server group *sg1*. Type the following command:

   23x0# **set authentication dot1x ssid mycorp * pass-through sg1**

4. Save the configuration:

   ```
   WSS-20 save config
   success: configuration saved.
   ```

(For information about setting up RADIUS servers for remote authentication, see "Configuring Communication with RADIUS," on page 477.)

Enabling PEAP-MS-CHAP-V2 Authentication

The following example illustrates how to enable local PEAP-MS-CHAP-V2 authentication for all 802.1X network users. This example includes local usernames, passwords, and membership in a VLAN. This example includes one username and an optional attribute for session-timeout in seconds. Because the WSS switch requires a certificate for authentication, configuration of a self-signed certificate is shown.

1. To set authentication for all 802.1X users of SSID *thiscorp*, type the following command:

   23x0# **set authentication dot1x ssid thiscorp * peap-mschapv2 local**

2. To add user Natasha to the local database on the WSS switch, type the following command:

   23x0# **set user Natasha password moon**

3. To assign Natasha to a VLAN named *red*, type the following command:

   23x0# **set user Natasha attr vlan-name red**

4. To assign Natasha a session timeout value of 1200 seconds, type the following command:

   23x0# **set user Natasha attr session-timeout 1200**

5. To generate a public-private key pair and a self-signed EAP certificate, type the following commands:

   23x0# **crypto generate key eap 1024**
   key pair generated

   23x0# **crypto generate self-signed eap**
   Country Name: **US**
   State Name: **CA**
   Locality Name: **campus1**
   Organizational Name: **Example**
   Organizational Unit: **IT**
   Common Name: **WSS33**
   Email Address: **admin@example.com**
   Unstructured Name: **wiring closet 22**

6. Save the configuration:

   WSS-20 **save config**
   success: configuration saved.

(For information about encryption keys and certificates, see "Managing Keys and Certificates," on page 379.)

Enabling PEAP-MS-CHAP-V2 Offload

The following example illustrates how to enable PEAP-MS-CHAP-V2 offload. In this example, all EAP processing is offloaded from the RADIUS server, but MS-CHAP-V2 authentication and authorization are done through a RADIUS server. The MS-CHAP-V2 lookup matches users against the user list on a RADIUS server. Because the WSS switch requires a certificate for authentication, a self-signed certificate is shown in this example.

1. Configure the RADIUS server *r1* at IP address 10.1.1.1 with the string *starry* for the key. Type the following command:

   23x0# **set radius server r1 address 10.1.1.1 key starry**

2. Configure the server group *sg1* with member *r1*. Type the following command:

   23x0# **set server group sg1 members r1**

3. Enable all 802.1X users of SSID *thiscorp* using PEAP-MS-CHAP-V2 to authenticate MS-CHAP-V2 on server group *sg1*. Type the following command:

   23x0# **set authentication dot1x ssid thiscorp * peap-mschapv2 sg1**

4. To generate a public-private key pair and a self-signed EAP certificate, type the following commands:

   23x0# **crypto generate key eap 1024**
   key pair generated

   23x0# **crypto generate self-signed eap**
   Country Name: **US**
   State Name: **CA**
   Locality Name: **campus1**
   Organizational Name: **Example**
   Organizational Unit: **IT**
   Common Name: **WSS6**
   Email Address: **admin@example.com**
   Unstructured Name: **wiring closet 55**

5. Save the configuration:

   WSS-20 **save config**
   success: configuration saved.

Combining 802.1X Acceleration with Pass-Through Authentication

The following example illustrates how to enable PEAP-MS-CHAP-V2 offload for the marketing (*mktg*) group and RADIUS pass-through authentication for members of engineering. This example assumes that engineering members are using DNS-style naming, such as is used with EAP-TLS. An WSS server certificate is also required. Because the WSS switch requires a certificate for authentication, a self-signed certificate is shown in this example.

1. Configure the RADIUS server *r1* at IP address 10.1.1.1 with the string *starry* for the key. Type the following command:

   23x0# **set radius server r1 address 10.1.1.1 key starry**

2. Configure the server group *sg1* with member *r1*. Type the following command:

   23x0# **set server group sg1 members r1**

3. To authenticate all 802.1X users of SSID *bobblehead* in the group *mktg* using PEAP on the WSS switch and MS-CHAP-V2 on server *sg1*, type the following command:

   23x0# **set authentication dot1x ssid bobblehead mktg* peap-mschapv2 sg1**

4. To authenticate all 802.1X users of SSID *aircorp* in @eng.example.com through pass-through to *sg1*, type the following command:

   23x0# **set authentication dot1x ssid aircorp *@eng.example.com pass-through sg1**

5. To generate a public-private key pair and a self-signed EAP certificate, type the following commands:

   23x0# **crypto generate key eap 1024**
   key pair generated

   23x0# **crypto generate self-signed eap**
   Country Name: **US**
   State Name: **CA**
   Locality Name: **campus1**
   Organizational Name: **Example**
   Organizational Unit: **IT**
   Common Name: **WSS 33**
   Email Address: **admin@example.com**
   Unstructured Name: **wiring closet south campus**

6. Save the configuration:

   WSS-20 **save config**
   success: configuration saved.

Overriding AAA-Assigned VLANs

The following example shows how to change the VLAN access of wireless users in an organization housed in multiple buildings.

Suppose the wireless users on the faculty of a college English department have offices in building A and are authorized to use that building's *bldga-prof-* VLANs. These users also teach classes in building B. Because you do not want to tunnel these users back to building A from building B when they use their wireless laptops in class, you configure the location policy on the WSS switch to redirect them to the *bldgb-eng* VLAN.

You also want to allow writing instructors normally authorized to use any *-techcomm* VLAN in the college to access the network through the *bldgb-eng* VLAN when they are in building B.

1. Redirect *bldga-prof-* VLAN users to the VLAN *bldgb-eng*:

   ```
   23x0# set location policy permit vlan bldgb-eng if vlan eq
   bldga-prof-*
   ```

2. Allow writing instructors from *-techcomm* VLANs to use the *bldgb-eng* VLAN:

   ```
   23x0# set location policy permit vlan bldgb-eng if vlan eq
   *-techcomm
   ```

3. Display the configuration:

   ```
   23x0# show location policy
   Id Clauses
   ---------------------------------------------------
   1) permit vlan bldgb-teach if vlan eq bldga-prof-*
   2) permit vlan bldgb-eng if vlan eq *-techcomm
   ```

4. Save the configuration:

   ```
   WSS-20 save config
   success: configuration saved.
   ```

Configuring Communication with RADIUS

RADIUS Overview 477
Before You Begin 479
Configuring RADIUS Servers 479
Configuring RADIUS Server Groups 483
RADIUS and Server Group Configuration Scenario 487

For a list of the standard and extended RADIUS attributes and Nortel vendor-specific attributes (VSAs) supported by WSS Software, see "Supported RADIUS Attributes," on page 599.

RADIUS Overview

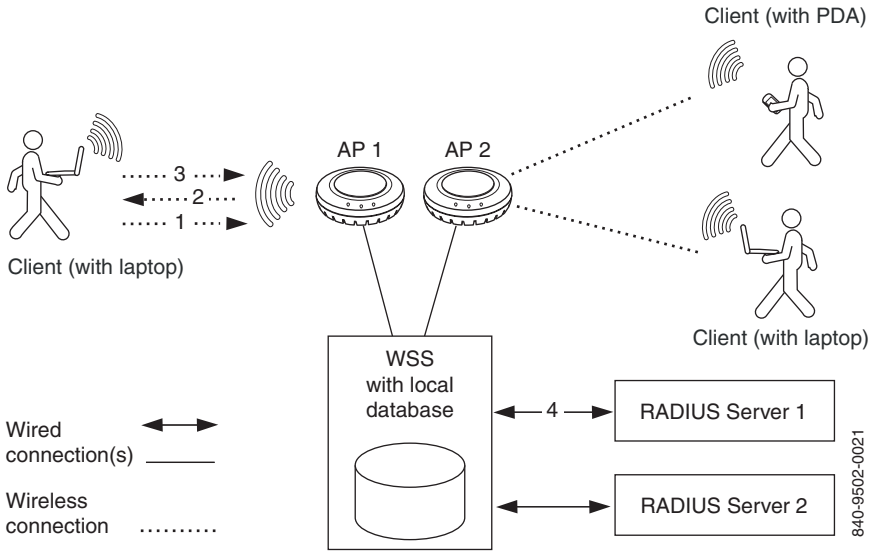
Remote Authentication Dial-In User Service (RADIUS) is a distributed client-server system. RADIUS servers provide a repository for all usernames and passwords, and can manage and store large groups of users.

RADIUS servers store user profiles, which include usernames, passwords, and other AAA attributes. You can use authorization attributes to authorize users for a type of service, for appropriate servers and network segments through VLAN assignments, for packet filtering by access control lists (ACLs), and for other services during a session.

You must include RADIUS servers in a server group before you can access them. (See "Configuring RADIUS Server Groups" on page 483.)

Figure 20 on page 478 illustrates the interactions between wireless users (clients), AP access ports, an WSS switch, and its attached RADIUS servers when the clients attempt access.

Figure 20. Wireless Client, AP access port, WSS Switch, and RADIUS Servers



In the example shown in Figure 20, the following events occur:

1. The wireless user (client) requests an IEEE 802.11 association from the AP access port.
2. After the AP access point creates the association, the WSS switch sends an Extensible Authentication Protocol (EAP) identity request to the client.
3. The client sends an EAP identity response.
4. From the EAP response, the WSS switch gets the client's username. The WSS switch then searches its AAA configuration, attempting to match the client's username against the user wildcards in the AAA configuration.

   When a match is found, the methods specified by the matching AAA command in the WSS configuration file indicate how the client is to be authenticated, either locally on the WSS switch, or through a RADIUS server group.
5. If the client does not support 802.1X, WSS Software attempts to perform MAC authentication for the client instead. In this case, if the switch's configuration contains a **set authentication mac** command that matches the client's MAC address, WSS Software uses the method specified by the command. Otherwise, WSS Software uses local MAC authentication by default.

   (For information about MAC client authentication, see "Configuring MAC Authentication and Authorization" on page 427.)

Before You Begin

To ensure that you can contact the RADIUS servers you plan to use for authentication, send the **ping** command to each one to verify connectivity.

ping *ip-address*

You can then set up communication between the WSS switch and each RADIUS server group.

Configuring RADIUS Servers

An authentication server authenticates each client with access to a switch port before making available any services offered by the switch or the wireless network. The authentication server can reside either in the local database on the WSS switch or on a remote RADIUS server.

When a RADIUS server is used for authentication, you must configure RADIUS server parameters. For each RADIUS server, you must, at a minimum, set the server name, the password (key), and the IP address. You can include any or all of the other optional parameters. You can set some parameters globally for the RADIUS servers.

For RADIUS servers that do not explicitly set their own dead time and timeout timers and transmission attempts, WSS Software sets the following values by default:

- Dead time—0 (zero) minutes (The WSS switch does not designate unresponsive RADIUS servers as unavailable.)
- Transmission attempts—3
- Timeout (WSS wait for a server response)—5 seconds

When WSS Software sends an authentication or authorization request to a RADIUS server, WSS Software waits for the amount of the RADIUS timeout for the server to respond. If the server does not respond, WSS Software retransmits the request. WSS Software sends the request up to the number of retransmits configured. (The retransmit setting specifies the total number of attempts, including the first attempt.) For example, using the default values, WSS Software sends a request to a server up to three times, waiting 5 seconds between requests.

If a server does not respond before the last request attempt times out, WSS Software holds down further requests to the server, for the duration of the dead time. For example, if you set the dead time to 5 minutes, WSS Software stops sending requests to the unresponsive server for 5 minutes before reattempting to use the server.

During the holddown, it is as if the *dead* RADIUS server does not exist. WSS Software skips over any dead RADIUS servers to the next *live* server, or on to the next method if no more live servers are available, depending on your configuration. For example, if a RADIUS server group is the primary authentication method and **local** is the secondary method, WSS Software fails over to the local method if all RADIUS servers in the server group are unresponsive and have entered the dead time.

For failover authentication or authorization to work promptly, Nortel recommends that you change the dead time to a value other than 0. With the default setting, the dead time is never invoked and WSS Software does not hold down requests to unresponsive RADIUS servers. Instead, WSS Software attempts to send each new authentication or authorization request to a server even if the server is thought to be unresponsive. This behavior can cause authentication or authorization failures on clients because WSS Software does not fail over to the local method soon enough and the clients eventually time out.

Configuring Global RADIUS Defaults

You can change RADIUS values globally and set a global password (key) with the following command. The key *string* is the shared secret that the WSS switch uses to authenticate itself to the RADIUS server.

set radius {**deadtime** *minutes* | **key** *string* | **retransmit** *number* | **timeout** *seconds*}

(To override global settings for individual RADIUS servers, use the **set radius server** command. See "Configuring Individual RADIUS Servers" on page 482.)

For example, the following commands set the dead-time timer to 10 minutes and set the password to *r8gney* for all RADIUS servers in the WSS configuration:

```
23x0# set radius deadtime 10
success: change accepted.

23x0# set radius key r8gney
success: change accepted.
```

To reset global RADIUS server settings to their factory defaults, use the following command:

clear radius {**deadtime** | **key** | **retransmit** | **timeout**}

For example, the following command resets the dead-time timer to 0 minutes on all RADIUS servers in the WSS configuration:

```
23x0# clear radius deadtime
success: change accepted.
```

Setting the System IP Address as the Source Address

By default, RADIUS packets leaving the WSS switch have the source IP address of the outbound interface on the switch. This source address can change when routing conditions change. If you have set a system IP address for the WSS switch, you can use it as a permanent source address for the RADIUS packets sent by the switch.

To set the WSS system IP address as the address of the RADIUS client, type the following command:

```
23x0# set radius client system-ip
success: change accepted.
```

To remove the WSS switch's system IP address from use as the source address in RADIUS client requests from the switch to its RADIUS server(s), type the following command:

```
23x0# clear radius client system-ip
success: change accepted.
```

The command causes the WSS to select a source interface address based on information in its routing table as the RADIUS client address.

Configuring Individual RADIUS Servers

You must set up a name and IP address for each RADIUS server. To configure a RADIUS server, use the following command:

set radius server *server-name* **[address** *ip-address*] **[key** *string*]

The server name must be unique for this RADIUS server on this WSS switch. The key (password) *string* is the shared secret that the WSS switch uses to authenticate itself to the RADIUS server. Do not use the same name for a RADIUS server and a RADIUS server group.

For example, the following command names a RADIUS server *rs1* with the IP address 192.168.0.2 and the key *testing123*:

```
2370# set radius server rs1 address 192.168.0.2 key testing123
success: change accepted.
```

You can configure multiple RADIUS servers. When you define server names and keys, case is significant. For example:

```
2370# set radius server rs1 address 10.6.7.8 key seCret
success: change accepted.

2370# set radius server rs2 address 10.6.7.9 key BigSecret
success: change accepted.
```



Note. You must provide RADIUS servers with names that are unique. To prevent confusion, Nortel recommends that RADIUS server names differ in ways other than case. For example, avoid naming two servers *RS1* and *rs1*.

(You can configure additional parameters with **set radius server**, such as the UDP ports used for AAA services and the timeout period. For details, see the *Nortel Mobility System Software Command Reference*.)

You must configure RADIUS servers into server groups before you can access them. For information on creating server groups, see "Configuring RADIUS Server Groups" on page 483.

Deleting RADIUS Servers

To remove a RADIUS server from the WSS configuration, use the following command:

clear radius server *server-name*

Configuring RADIUS Server Groups

A server group is a named group of up to four RADIUS servers. Before you can use a RADIUS server for authentication, you must first create a RADIUS server group and add the RADIUS server to that group. You can also arrange load balancing, so that authentications are spread out among servers in the group. You must declare *all* members of a server group, in contact order, when you create the group.

Once the group is configured, you can use a server group name as the AAA method with the **set authentication** and **set accounting** commands. (See Chapter , “Configuring AAA for Administrative and Local Access,” on page 51 and Chapter , “Configuring AAA for Network Users,” on page 401.)

Subsequently, you can change the members of a group or configure load balancing.

If you add or remove a RADIUS server in a server group, all the RADIUS dead timers for that server group are reset to the global default.

Creating Server Groups

To create a server group, you must first configure the RADIUS servers with their addresses and any optional parameters. After configuring RADIUS servers, type the following command:

set server group *group-name* **members** *server-name1* [*server-name2*] [*server-name3*] [*server-name4*]

For example, to create a server group called *shorebirds* with the RADIUS servers *heron, egret*, and *sandpiper*, type the following commands:

```
23x0# set radius server egret address 192.168.253.1 key apple
23x0# set radius server heron address 192.168.253.2 key pear
23x0# set radius server sandpiper address 192.168.253.3 key plum
23x0# set server group shorebirds members egret heron sandpiper
```

In this example, a request to *shorebirds* results in the RADIUS servers being contacted in the order that they are listed in the server group configuration, first *egret*, then *heron*, then *sandpiper*. You can change the RADIUS servers in server groups at any time. (See "Adding Members to a Server Group" on page 485.)



Note. Any RADIUS servers that do not respond are marked *dead* (unavailable) for a period of time. The unresponsive server is skipped over, as though it did not exist, during its dead time. Once the dead time elapses, the server is again a candidate for receiving requests. To change the default dead-time timer, use the **set radius** or **set radius server** command.

Ordering Server Groups

You can configure up to four methods for authentication, authorization, and accounting (AAA). AAA methods can be the local database on the WSS switch and/or one or more RADIUS server groups. You set the order in which the WSS switch attempts the AAA methods by the order in which you enter the methods in CLI commands.

In most cases, if the first method results in a pass or fail, the evaluation is final. If the first method does not respond or results in an error, the WSS switch tries the second method and so on.

However, if the local database is the first method in the list, followed by a RADIUS server group, the WSS switch responds to a failed search of the database by sending a request to the following RADIUS server group. This exception is called local override.

For more information, see "AAA Methods for IEEE 802.1X and Web Network Access" on page 412.

Configuring Load Balancing

You can configure the WSS switch to distribute authentication requests across RADIUS servers in a server group, which is called load balancing. Distributing the authentication process across multiple RADIUS servers significantly reduces the load on individual servers while increasing resiliency on a systemwide basis.

When you configure load balancing, the first client's RADIUS requests are directed to the first server in the group, the second client's RADIUS requests are directed to the second server in the group, and so on. When the last server in the group is reached, the cycle is repeated.



Note. WSS Software attempts to send accounting records to one RADIUS server, even if load balancing is configured.

To configure load balancing, use the following command:

set server group *group-name* **load-balance enable**

For example, to configure RADIUS servers *pelican* and *seagull* as the server group *swampbirds* with load balancing:

1. Configure the members of a server group by typing the following command:

   ```
   23x0# set server group swampbirds members pelican seagull
   success: change accepted.
   ```

2. Enable load balancing by typing the following command:

   ```
   23x0# set server group swampbirds load-balance enable
   success: change accepted.
   ```

The following command disables load balancing for a server group:

clear server group *group-name* **load-balance**

Adding Members to a Server Group

To add RADIUS servers to a server group, type the following command:

set server group *group-name* **members** *server-name1* [*server-name2*] [*server-name3*] [*server-name4*]]

The keyword **members** lists the RADIUS servers contained in the named server group. A server group can contain between one and four RADIUS servers. This command accepts any RADIUS servers as the current set of servers. To change the server members, you must reenter all of them.

For example, to add RADIUS server *coot* to server group *shorebirds*:

1. Determine the server group by typing the following command:

   ```
   23x0# show aaa
   Radius Servers
   Server                    Addr            Ports   T/o Tries Dead
   State
   ------------------------------------------------------------------
   ----
   sandpiper            192.168.253.3   1812 1813  5    3    0    UP
   heron                192.168.253.1   1812 1813  5    3    0    UP
   coot                 192.168.253.4   1812 1813  5    3    0    UP
   ```

```
egret              192.168.253.2   1812 1813  5    3    0
UP

Server groups
    shorebirds (load-balanced): sandpiper heron egret
```

The RADIUS server *coot* is configured but not part of the server group *shorebirds.*

2 To add RADIUS server *coot* as the last server in the server group *shorebirds*, type the following command:

```
23x0# set server group shorebirds members sandpiper heron egret coot
success: change accepted.
```

Deleting a Server Group

To remove a server group, type the following command:

clear server group *group-name*

For example, to delete the server group *shorebirds*, type the following command:

```
23x0# clear server group shorebirds
success: change accepted.
```

The members of the group remain configured, although no server groups are shown:

```
23x0# show aaa
Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=0 key=(null) author-pass=(null)

Radius Servers
Server                  Addr           Ports   T/o Tries Dead State
-------------------------------------------------------------------
sandpiper            192.168.253.3   1812 1813  5    3    0    UP
heron                192.168.253.1   1812 1813  5    3    0    UP
coot                 192.168.253.4   1812 1813  5    3    0    UP
egret                192.168.253.2   1812 1813  5    3    0    UP
Server groups
```

RADIUS and Server Group Configuration Scenario

The following example illustrates how to declare four RADIUS servers to an WSS switch and configure them into two load-balancing server groups, *swampbirds* and *shorebirds:*

1. Configure RADIUS servers. Type the following commands:

   23x0# **set radius server pelican address 192.168.253.11 key elm**

   23x0# **set radius server seagull address 192.168.243.12 key fir**

   23x0# **set radius server egret address 192.168.243.15 key pine**

   23x0# **set radius server sandpiper address 192.168.253.17 key oak**

2. Place two of the RADIUS servers into a server group called *swampbirds*. Type the following command:

   23x0# **set server group swampbirds members pelican seagull**

3. Enable load balancing for *swampbirds*. Type the following command:

   23x0# **set server group swampbirds load-balance enable**

4. Place the other RADIUS servers in a server group called *shorebirds*. Type the following command:

   23x0# **set server group shorebirds members egret pelican sandpiper**

5 Enable load balancing for *shorebirds*. Type the following command:

```
23x0# set server group shorebirds load-balance enable
```

6 Display the configuration. Type the following command:

```
23x0# show aaa
Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=0 key=(null) author-pass=(null)

Radius Servers
Server                   Addr           Ports   T/o Tries Dead
State
-------------------------------------------------------------------
----
sandpiper           192.168.253.17  1812 1813  5    3    0    UP
seagull             192.168.243.12  1812 1813  5    3    0    UP
egret               192.168.243.15  1812 1813  5    3    0    UP
pelican             192.168.253.11  1812 1813  5    3    0    UP

Server groups
    swampbirds (load-balanced): pelican seagull
    shorebirds (load-balanced): egret pelican sandpiper
```

Managing 802.1X on the WSS Switch

Managing 802.1X on Wired Authentication Ports 489
Managing 802.1X Encryption Keys 491
Setting EAP Retransmission Attempts 495
Managing 802.1X Client Reauthentication 495
Managing Other Timers 499
Displaying 802.1X Information 502

Certain settings for IEEE 802.1X sessions on the WSS switch are enabled by default. For best results, change the settings only if you are aware of a problem with the WSS switch's 802.1X performance. For settings that you can reset with a **clear** command, WSS Software reverts to the default value.

See "Managing WEP Keys" on page 494 for information about changing the settings for Wired-Equivalent Privacy protocol (WEP) key rotation (rekeying).



Caution! 802.1X parameter settings are global for all SSIDs configured on the switch.

Managing 802.1X on Wired Authentication Ports

A wired authentication port is an Ethernet port that has 802.1X authentication enabled for access control. Like wireless users, users that are connected to an WSS switch by Ethernet wire can be authenticated before they can be authorized to use the network. One difference between a wired authenticated user and a *wireless* authenticated user is that data for wired users is not encrypted after the users are authenticated.

By default, 802.1X authentication is enabled for wired authenticated ports, but you can disable it. You can also set the port to unconditionally authorize, or unconditionally reject, all users.

Enabling and Disabling 802.1X Globally

The following command globally enables or disables 802.1X authentication on all wired authentication ports on an WSS switch:

set dot1x authcontrol {enable | disable}

The default setting is **enable**, which permits 802.1X authentication to occur as determined by the **set dot1X port-control** command for each wired authentication port. The **disable** setting forces all wired authentication ports to unconditionally authorize all 802.1X authentication attempts by users with an EAP success message.

To reenable 802.1X authentication on wired authentication ports, type the following command:

```
23x0# set dot1x authcontrol enable
success: dot1x authcontrol enabled.
```

Setting 802.1X Port Control

The following command specifies the way a wired authentication port or group of ports handles user 802.1X authentication attempts:

set dot1x port-control {forceauth | forceunauth | auto} *port-list*

The default setting is **auto**, which allows the WSS switch to process 802.1X authentication normally according to the authentication configuration. Alternatively, you can set a wired authentication port or ports to either unconditionally authenticate or unconditionally reject all users.

For example, the following command forces port 19 to unconditionally authenticate all 802.1X authentication attempts with an EAP success message:

```
23x0# set dot1x port-control forceauth 19
success: authcontrol for 19 is set to FORCE-AUTH.
```

Similarly, the following command forces port 12 to unconditionally reject any 802.1X attempts with an EAP failure message:

```
23x0# set dot1x port-control forceunauth 12
success: authcontrol for 12 is set to FORCE-UNAUTH.
```

The **set dot1x port-control** command is overridden by the **set dot1x authcontrol** command. The **clear dot1x port-control** command returns port control to the default **auto** value.

Type the following command to reset port control for all wired authentication ports:

```
23x0# clear dot1x port-control
success: change accepted.
```

Managing 802.1X Encryption Keys

By default, the WSS switch sends encryption key information to a wireless supplicant (client) in an Extensible Authentication Protocol over LAN (EAPoL) packet after authentication is successful. You can disable this feature or change the time interval for key transmission.

The secret Wired-Equivalent Privacy protocol (WEP) keys used by WSS Software on AP access ports for broadcast communication on a VLAN are automatically rotated (rekeyed) every 30 minutes to maintain secure packet transmission. You can disable WEP key rotation for debugging purposes, or change the rotation interval.

Enabling 802.1X Key Transmission

The following command enables or disables the transmission of key information to the supplicant (client) in EAPoL key messages, after authentication:

set dot1x key-tx {enable | disable}

Key transmission is enabled by default.

The WSS switch sends EAPoL key messages after successfully authenticating the supplicant (client) and receiving authorization attributes for the client. If the client is using dynamic WEP, the EAPoL Key messages are sent immediately after authorization.

Type the following command to reenable key transmission:

```
23x0# set dot1x key-tx enable
success: dot1x key transmission enabled.
```

Configuring 802.1X Key Transmission Time Intervals

The following command sets the number of seconds the WSS switch waits before retransmitting an EAPoL packet of key information:

set dot1x tx-period *seconds*

The default is 5 seconds. The range for the retransmission interval is from 1 to 65,535 seconds. For example, type the following command to set the retransmission interval to 300 seconds:

```
23x0# set dot1x tx-period 300
success: dot1x tx-period set to 300.
```

Type the following command to reset the retransmission interval to the 5-second default:

```
23x0# clear dot1x tx-period
success: change accepted.
```

Managing WEP Keys

Wired-Equivalent Privacy (WEP) is part of the system security of 802.1X. WSS Software uses WEP to provide confidentiality to packets as they are sent over the air. WEP operates on the AP access port.

WEP uses a secret key shared between the communicators. WEP rekeying increases the security of the network. New unicast keys are generated every time a client performs 802.1X authentication.

The rekeying process can be performed automatically on a periodic basis. By setting the Session-Timeout RADIUS attribute, you make the reauthentication transparent to the client, who is unaware that reauthentication is occurring. A good value for Session-Timeout is 30 minutes.

WEP broadcast rekeying causes the broadcast and multicast keys for WEP to be rotated every WEP rekey period for each radio to each connected VLAN. The WSS switch generates the new broadcast and multicast keys and pushes the keys to the clients through EAPoL key messages. WEP keys are case-insensitive.

Use the **set dot1x wep-rekey** and the **set dot1x wep-rekey-period** commands to enable WEP key rotation and configure the time interval for WEP key rotation.

Configuring 802.1X WEP Rekeying

WEP rekeying is enabled by default on the WSS switch. Disable WEP rekeying only if you need to debug your 802.1X network.

Use the following command to disable WEP rekeying for broadcast and multicast keys:

```
23x0# set dot1x wep-rekey disable
success: wep rekeying disabled
```



Note. Reauthentication is *not* required for using this command. Broadcast and multicast keys are always rotated at the same time, so all members of a given radio and VLAN receive the new keys at the same time.

To reenable WEP rekeying, type the following command:

```
23x0# set dot1x wep-rekey enable
success: wep rekeying enabled
```

Configuring the Interval for WEP Rekeying

The following command sets the interval for rotating the WEP broadcast and multicast keys:

set dot1x wep-rekey-period *seconds*

The default is 1800 seconds (30 minutes). You can set the interval from 30 to 1,641,600 seconds (19 days). For example, type the following command to set the WEP-rekey period to 900 seconds:

```
23x0# set dot1x wep-rekey-period 900
success: dot1x wep-rekey-period set to 900
```

Setting EAP Retransmission Attempts

The following command sets the maximum number of times the WSS switch retransmits an 802.1X-encapsulated EAP request to the supplicant (client) before it times out the authentication session:

set dot1x max-req *number-of-retransmissions*

The default number of retransmissions is 2. You can specify from 0 to 10 retransmit attempts. For example, type the following command to set the maximum number of retransmission attempts to 3:

```
23x0# set dot1x max-req 3
success: dot1x max request set to 3.
```

To reset the number of retransmission attempts to the default setting, type the following command:

```
23x0# clear dot1x max-req
success: change accepted.
```



Note. To support SSIDs that have both 802.1X and static WEP clients, WSS Software sends a maximum of two ID requests, even if this parameter is set to a higher value. Setting the parameter to a higher value does affect all other types of EAP messages.

Managing 802.1X Client Reauthentication

Reauthentication of 802.1X wireless supplicants (clients) is enabled on the WSS switch by default. By default, the WSS switch waits 3600 seconds (1 hour) between authentication attempts. You can disable reauthentication or change the defaults.

Enabling and Disabling 802.1X Reauthentication

The following command enables or disables the reauthentication of supplicants (clients) by the WSS switch:

set dot1x reauth {enable | disable}

Reauthentication is enabled by default.

Type the following command to reenable reauthentication of clients:

```
23x0# set dot1x reauth enable
success: dot1x reauthentication enabled.
```

Setting the Maximum Number of 802.1X Reauthentication Attempts

The following command sets the number of reauthentication attempts that the WSS switch makes before the supplicant (client) becomes unauthorized:

set dot1x reauth-max *number-of-attempts*

The default number of reauthentication attempts is 2. You can specify from 1 to 10 attempts. For example, type the following command to set the number of authentication attempts to 8:

```
23x0# set dot1x reauth-max 8
success: dot1x max reauth set to 8.
```

Type the following command to reset the maximum number of reauthorization attempts to the default:

```
23x0# clear dot1x reauth-max
success: change accepted.
```



Note. If the number of reauthentications for a wired authentication client is greater than the maximum number of reauthentications allowed, WSS Software sends an EAP failure packet to the client and removes the client from the network. However, WSS Software does not remove a wireless client from the network under these circumstances.

Setting the 802.1X Reauthentication Period

The following command configures the number of seconds that the WSS switch waits before attempting reauthentication:

set dot1x reauth-period *seconds*

The default is 3600 seconds (1 hour). The range is from 60 to 1,641,600 seconds (19 days). This value can be overridden by user authorization parameters.

WSS Software reauthenticates dynamic WEP clients based on the reauthentication timer. WSS Software also reauthenticates WPA clients if the clients use the WEP-40 or WEP-104 cipher. For each dynamic WEP client or WPA client using a WEP cipher, the reauthentication timer is set to the lesser of the global setting or the value returned by the AAA server with the rest of the authorization attributes for that client.

For example, type the following command to set the number of seconds to 100 before reauthentication is attempted:

```
23x0# set dot1x reauth-period 100
success: dot1x auth-server timeout set to 100.
```

Type the following command to reset the default timeout period:

```
23x0# clear dot1x reauth-period
success: change accepted.
```

Setting the Bonded Authentication Period

The following command sets the Bonded Authentication™ (bonded authentication) period, which is the number of seconds WSS Software retains session information for an authenticated machine while waiting for the 802.1X client on the machine to start (re)authentication for the user.

Normally, the Bonded Authentication period needs to be set only if the network has Bonded Authentication clients that use dynamic WEP, or use WEP-40 or WEP-104 encryption with WPA or RSN. These clients can be affected by the 802.1X reauthentication parameter or the RADIUS Session-Timeout parameter.

To set the Bonded Authentication period, use the following command:

set dot1x bonded-period *seconds*

The Bonded Authentication period applies only to 802.1X authentication rules that contain the **bonded** option.

To reset the Bonded Authentication period to its default value, use the following command:

clear dot1x max-req

(For more information about Bonded Authentication, see "Binding User Authentication to Machine Authentication" on page 421.)

Managing Other Timers

By default, the WSS switch waits 60 seconds before responding to a client whose authentication failed, and times out a request to a RADIUS server or an authentication session with a client after 30 seconds. You can modify these defaults.

Setting the 802.1X Quiet Period

The following command configures the number of seconds an WSS switch remains quiet and does not respond to a supplicant (client) after a failed authentication:

set dot1x quiet-period *seconds*

The default is 60 seconds. The acceptable range is from 0 to 65,535 seconds.

For example, type the following command to set the quiet period to 300 seconds:

```
23x0# set dot1x quiet-period 300
success: dot1x quiet period set to 300.
```

Type the following command to reset the 802.1X quiet period to the default:

```
23x0# clear dot1x quiet-period
success: change accepted.
```

Setting the 802.1X Timeout for an Authorization Server

Use this command to configure the number of seconds before the WSS switch times out a request to a RADIUS authorization server.

set dot1x timeout auth-server *seconds*

The default is 30 seconds. The range is from 1 to 65,535 seconds.

For example, type the following command to set the authorization server timeout to 60 seconds:

```
23x0# set dot1x timeout auth-server 60
success: dot1x auth-server timeout set to 60.
```

To reset the authorization server timeout to the default, type the following command:

```
23x0# clear dot1x timeout auth-server
success: change accepted.
```

Setting the 802.1X Timeout for a Client

Use the following command to set the number of seconds before the WSS switch times out an authentication session with a supplicant (client):

set dot1x timeout supplicant *seconds*

The default is 30 seconds. The range of time is from 1 to 65,535 seconds.

For example, type the following command to set the number of seconds for a timeout to 300:

```
23x0# set dot1x timeout supplicant 300
success: dot1x supplicant timeout set to 300.
```

Type the following command to reset the timeout period:

```
23x0# clear dot1x timeout supplicant
success: change accepted.
```

Displaying 802.1X Information

This command displays 802.1X information for clients, statistics, VLANs, and configuration.

show dot1x {clients | stats | config}

- **show dot1x clients** displays the username, MAC address, VLAN, and state of active 802.1X clients.
- **show dot1x config** displays a summary of the current configuration.
- **show dot1x stats** displays global 802.1X statistical information associated with connecting and authenticating.

Viewing 802.1X Clients

Type the following command to display active 802.1X clients:

23x0# **show dot1x clients**

MAC Address	State	Vlan	Identity
00:20:a6:48:01:1f	Connecting	(unknown)	
00:05:3c:07:6d:7c	Authenticated	vlan-it	EXAMPLE\smith
00:05:5d:7e:94:83	Authenticated	vlan-eng	EXAMPLE\jgarcia
00:02:2d:86:bd:38	Authenticated	vlan-eng	wong@exAPl.com
00:05:5d:7e:97:b4	Authenticated	vlan-eng	EXAMPLE\hosni
00:05:5d:7e:98:1a	Authenticated	vlan-eng	EXAMPLE\tsmith
00:0b:be:a9:dc:4e	Authenticated	vlan-pm	havel@nrtl.com
00:05:5d:7e:96:e3	Authenticated	vlan-eng	EXAMPLE\geetha
00:02:2d:6f:44:77	Authenticated	vlan-eng	EXAMPLE\tamara
00:05:5d:7e:94:89	Authenticated	vlan-eng	EXAMPLE\nwong
00:06:80:00:5c:02	Authenticated	vlan-eng	EXAMPLE\hhabib
00:02:2d:6a:de:f2	Authenticated	vlan-pm	smith@exAPl.com
00:02:2d:5e:5b:76	Authenticated	vlan-pm	EXAMPLE\natasha
00:02:2d:80:b6:e1	Authenticated	vlan-cs	jjg@exAPl.com
00:30:65:16:8d:69	Authenticated	vlan-wep	MAC authenticated
00:02:2d:64:8e:1b	Authenticated	vlan-eng	EXAMPLE\jose

Viewing the 802.1X Configuration

Type the following command to display the 802.1X configuration:

```
23x0# show dot1x config

            802.1X user policy
          ----------------------
 'EXAMPLE\pc1' on ssid 'mycorp' doing EAP-PEAP (EAP-MSCHAPv2)
 'EXAMPLE\bob' on ssid 'mycorp' doing EAP-PEAP (EAP-MSCHAPv2) (bonded)

       802.1X parameter                setting
       ----------------                -------
       supplicant timeout              30
       auth-server timeout             30
       quiet period                    5
       transmit period                 5
       reauthentication period         3600
       maximum requests                2
       key transmission                enabled
       reauthentication                enabled
       authentication control          enabled
       WEP rekey period                1800
       WEP rekey                       enabled
       Bonded period                   60


       port 5, authcontrol: auto, max-sessions: 16
       port 6, authcontrol: auto, max-sessions: 1
       port 7, authcontrol: auto, max-sessions: 1
       port 8, authcontrol: auto, max-sessions: 1
       port 9, authcontrol: auto, max-sessions: 1
       port 10, authcontrol: auto, max-sessions: 1
       port 11, authcontrol: auto, max-sessions: 1
       port 12, authcontrol: auto, max-sessions: 1
       port 13, authcontrol: auto, max-sessions: 1
       port 14, authcontrol: auto, max-sessions: 1
       port 15, authcontrol: auto, max-sessions: 1
       port 16, authcontrol: auto, max-sessions: 1
       port 22, authcontrol: auto, max-sessions: 16
```

Viewing 802.1X Statistics

Type the following command to display 802.1X statistics about connecting and authenticating:

```
23x0# show dot1x stats
        802.1X statistic                value
        ----------------                -----
        Enters Connecting:              709
        Logoffs While Connecting:       112
        Enters Authenticating:          467
        Success While Authenticating:   0
        Timeouts While Authenticating:  52
        Failures While Authenticating:  0
        Reauths While Authenticating:   0
        Starts While Authenticating:    31
        Logoffs While Authenticating:   0
        Starts While Authenticated:     85
        Logoffs While Authenticated:    1
        Bad Packets Received:           0
```

For information about the fields in the output, see the *Nortel Mobility System Software Command Reference.*

Managing Sessions

About the Session Manager 507
Displaying and Clearing Administrative Sessions 507
Displaying and Clearing Network Sessions 511

About the Session Manager

A session is a related set of communication transactions between an authenticated user (client) and the specific station to which the client is bound. Packets are exchanged during a session. An WSS switch supports the following kinds of sessions:

- **Administrative sessions**—A network administrator managing the WSS
- **Network sessions**—A network user exchanging traffic with a network through the WSS

The WSS session manager manages the sessions for each client, but does not examine the substance of the traffic.

Clearing (ending) a session deauthenticates the administrator or user from the session and disassociates wireless clients.

Displaying and Clearing Administrative Sessions

To display session information and statistics for a user with administrative access to the WSS switch, use the following command:

show sessions {admin | console | telnet [client]}

You can view all administrative sessions, or only the sessions of administrators with access to the WSS through a Telnet or SSH connection or the console port. You can also display information about administrative Telnet sessions from remote clients.

To clear administrative sessions, use the following command:

clear sessions {admin | console | telnet [client [*session-id*]]}



Caution! Clearing administrative sessions might cause your session to be cleared.

Displaying and Clearing All Administrative Sessions

To view information about the sessions of all administrative users, type the following command:

```
WSS-20> show sessions admin
Tty          Username                Time (s)    Type
-------      --------------------    --------    ----
tty0                                 3644        Console
tty2         tech                    6           Telnet
tty3         sshadmin                381         SSH

3 admin sessions
```

To clear the sessions of all administrative users, type the following command:

```
23x0# clear sessions admin
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```

Displaying and Clearing an Administrative Console Session

To view information about the user with administrative access to the WSS switch through a console plugged into the switch, type the following command:

```
WSS-20> show sessions console
Tty          Username                Time (s)    Type
-------      --------------------    --------    ----
tty0                                 5310        Console

1 console session
```

To clear the administrative sessions of a console user, type the following command:

```
23x0# clear sessions console
This will terminate manager sessions, do you wish to continue? (y|n) [y]y
```

Displaying and Clearing Administrative Telnet Sessions

To view information about administrative Telnet sessions, type the following command:

```
WSS-20> show sessions telnet
Tty          Username              Time (s)    Type
-------      --------------------  --------    ----
tty3         sshadmin              2099        SSH

1 telnet session
```

To clear the administrative sessions of Telnet users, type the following command:

```
23x0# clear sessions telnet
This will terminate manager sessions, do you wish to continue? (y|n) [y]y
```

Displaying and Clearing Client Telnet Sessions

To view administrative sessions of Telnet clients, type the following command:

```
23x0# show sessions telnet client
Session   Server Address     Server Port    Client Port
-------   --------------     -----------    -----------
0          192.168.1.81      23             48000
1           10.10.1.22       23             48001
```

To clear the administrative sessions of Telnet clients, use the following command:

clear sessions telnet [client [*session-id***]]**

You can clear all Telnet client sessions or a particular session. For example, the following command clears Telnet client session 1:

```
23x0# clear sessions telnet client 1
```

Displaying and Clearing Network Sessions

Use the following command to display information about network sessions:

show sessions network [user *user-wildcard* | **mac-addr** *mac-addr-wildcard* | **ssid** *ssid-name* | **vlan** *vlan-wildcard* | **session-id** *session-id* | **wired] [verbose]**

In most cases, you can display both summary and detailed (verbose) information for a session. For example, the following command displays summary information about all current network sessions:

```
23x0# show sessions network
User                            Sess  IP or MAC          VLAN            Port/
Name                             ID   Address            Name            Radio
------------------------------ ----  -----------------  --------------- -----
EXAMPLE\wong                      5*  192.168.12.100     vlan-eng         3/1
jose@example.com               5125*  192.168.12.141     vlan-eng         1/1
00:30:65:16:8d:69              4385*  192.168.19.199     vlan-wep         3/1
                                761   00:0b:be:15:46:56  (none)           1/2
                                763   00:02:2d:02:10:f5  (none)           1/1
5 sessions total
```

An asterisk (*) in the *Sess ID* field indicates a session that is currently active. (For more information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

(For information about getting detailed output, see "Displaying Verbose Network Session Information" on page 512.)

You can display and clear network sessions in the following ways:

- By the name of the user. (See "Displaying and Clearing Network Sessions by Username" on page 513.)
- By the MAC address of the user. (See "Displaying and Clearing Network Sessions by MAC Address" on page 514.)
- By the name of the VLAN to which the user belongs. (See "Displaying and Clearing Network Sessions by VLAN Name" on page 515.)
- By the local session ID. (See "Displaying and Clearing Network Sessions by Session ID" on page 516.)

Displaying Verbose Network Session Information

In the **show sessions network** commands, you can specify **verbose** to get more in-depth information.

For example, to display detailed information for all network sessions, type the following command:

```
WSS-20> show sessions network verbose

User                            Sess  IP or MAC         VLAN            Port/
Name                             ID  Address           Name            Radio
------------------------------ ----  ----------------- --------------- -----
EXAMPLE\wong                     5* 192.168.12.100    vlan-eng         3/1
Client MAC: 00:02:2c:64:8e:1b   GID: SESS-5-000430-835541-bab048c4
State: ACTIVE                  (prev AUTHORIZED)
now on: WSS 192.168.12.7, AP/radio  3/1, AP 00:0b:0e:00:05:ef, as of 02:43:03 ago

jose@example.com                5125* 192.168.12.141    vlan-eng        1/1
Client MAC: 00:01:2e:6e:ab:a5   GID: SESS-5125-000430-843069-2b7d0
State: ACTIVE                  (prev AUTHORIZED)
now on: WSS 192.168.12.7, AP/radio  1/1, AP 00:0b:0e:00:05:ff, as of 00:37:35 ago

00:30:65:16:8d:69              4385* 192.168.19.199    vlan-wep         3/1
Client MAC: 00:10:65:16:8d:69   GID: SESS-4385-000430-842879-bf7a7
State: ACTIVE                  (prev AUTHORIZED)
now on: WSS 192.168.12.7, AP/radio  3/1, AP 00:0b:0e:00:05:ef, as of 00:40:45 ago

                                761  00:0b:be:15:46:56 (none)           1/2
Client MAC: 00:0e:be:15:46:56   GID: SESS-761-000430-845313-671851
State: AUTH AND ASSOC          (prev AUTH,ASSOC REQ)
now on: WSS 192.168.12.7, AP/radio  1/2, AP 00:0b:0e:00:06:00, as of 00:00:11 ago

User                            Sess  IP or MAC         VLAN            Port/
Name                             ID  Address           Name            Radio
------------------------------ ----  ----------------- --------------- -----

                                  763  00:02:2d:02:10:f5 (none)           1/1
Client MAC: 00:02:0d:02:10:f5   GID: SESS-763-000430-845317-fb2c2d
State: AUTH AND ASSOC          (prev AUTH,ASSOC REQ)
now on: WSS 192.168.12.7, AP/radio  1/1, AP 00:0b:0e:00:05:ff, as of 00:00:07 ago

5 sessions total
```

Displaying and Clearing Network Sessions by Username

You can view sessions by a username or user wildcard. (For a definition of user globs and their format, see "User Wildcards" on page 39.)

To see all sessions for a specific user or for a group of users, type the following command:

show sessions network user *user-wildcard*

For example, the following command shows all sessions of users whose names begin with *E*:

```
23x0# show sessions network user E*
User                          Sess  IP or MAC        VLAN           Port/
Name                            ID  Address          Name           Radio
-------------------------------------------------------------------------
EXAMPLE\singh                  12* 192.168.12.185   vlan-eng       3/2
EXAMPLE\havel                  13* 192.168.12.104   vlan-eng       1/2

2 sessions match criteria (of 3 total)
```

Use the **verbose** keyword to see more information. For example, the following command displays detailed session information about nin@example.com:

```
2370> show sessions network user nin@example.com verbose
User                           Sess  IP or MAC          VLAN            Port/
Name                            ID  Address            Name            Radio
------------------------------ ----  ----------------- --------------- -----
nin@example.com                  5* 192.168.12.141    vlan-eng         1/1
Client MAC: 00:02:2d:6e:ab:a5   GID: SESS-5-000430-686792-d8b3c564
State: ACTIVE                 (prev AUTHORIZED)
now on: WSS 192.168.12.7, AP/radio  1/1, AP 00:0b:0e:00:05:fe, as of 00:23:32 ago

1 sessions match criteria (of 10 total)
```

To clear all the network sessions of a user or group of users, use the following command:

clear sessions network user *user-wildcard*

For example, the following command clears the sessions of users named Bob:

```
2370# clear sessions network user Bob*
```

Displaying and Clearing Network Sessions by MAC Address

You can view sessions by MAC address or MAC address wildcard. (For a definition of MAC address globs and their format, see "MAC Address Wildcards" on page 39.) To view session information for a MAC address or set of MAC addresses, type the following command:

show sessions network mac-addr *mac-addr-wildcard*

For example, the following command displays the sessions for MAC address 01:05:5d:7e:98:1a:

```
2370> show sessions net mac-addr 01:05:5d:7e:98:1a
User                          Sess  IP or MAC         VLAN            Port/
Name                            ID  Address           Name              Radio
--------------------------- ----  --------------- ------------ -----
EXAMPLE\havel                  13* 192.168.12.104   vlan-eng     1/2
```

To clear all the network sessions for a MAC address or set of MAC addresses, use the following command:

clear sessions network mac-addr *mac-addr-wildcard*

For example, to clear all sessions for MAC address 00:01:02:04:05:06, type the following command:

```
2370# clear sessions network mac-addr 00:01:02:04:05:06
```

Displaying and Clearing Network Sessions by VLAN Name

You can view all session information for a specific VLAN or VLAN wildcard. (For a definition of VLAN globs and their format, see "VLAN Wildcards" on page 40.)

To see all network sessions information for a VLAN or set of VLANs, type the following command:

show sessions network vlan *vlan-wildcard*

For example, the following command displays the sessions for VLAN *west*:

```
2370> show sessions network vlan west

User                            Sess  IP or MAC         VLAN            Port/
Name                             ID   Address           Name            Radio
------------------------------ ----  ----------------- --------------- -----
EXAMPLE\tamara                   8* 192.168.12.174     west              1/1
host/laptop.example.com         11* 192.168.12.164     west              2/1
EXAMPLE\havel                   17* 192.168.12.195     west              1/2
EXAMPLE\jose                    20* 192.168.12.171     west              1/2
EXAMPLE\geetha                  21* 192.168.12.169     west              3/2
```

To clear the sessions on a VLAN or set of VLANs, use the following command:

clear sessions network vlan *vlan-wildcard*

For example, the following command clears the sessions of all users on VLAN *red*:

```
2370# clear sessions network vlan red
```

Displaying and Clearing Network Sessions by Session ID

You can display information about a session by session ID. To find local session IDs, enter the **show sessions** command. You can view more detailed information for an individual session, including authorization parameters and, for wireless sessions, packet and radio statistics.

For example, to display information about session 27, type the following command:

```
2370> show session network session-id 27
Global Id: SESS-27-000430-835586-58dfe5a
State: ACTIVE
Port/Radio: 3/1
MAC Address: 00:00:2d:6f:44:77
User Name: EXAMPLE\ethan
IP Address: 192.168.142.170
Vlan Name: vlan-eng
Tag: 1
Session Timeout: 1800
Authentication Method: PEAP, using server 192.168.142.7
Session statistics as updated from AP:
Unicast packets in: 653
Unicast bytes in: 46211
Unicast packets out: 450
Unicast bytes out: 50478
Multicast packets in: 317
Multicast bytes in: 10144
Number of packets with encryption errors: 0
Number of bytes with encryption errors: 0
Last packet data rate: 2
Last packet signal strength: -67 dBm
Last packet data S/N ratio: 55
```

(For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

The **verbose** option is not available with the **show sessions network session-id** command.

To clear network sessions by session ID, type the following command with the appropriate local session ID number.

clear sessions network session-id *session-id*

For example, the following command deletes network session 9:

```
2370# clear sessions network session-id 9

SM Apr 11 19:53:38 DEBUG SM-STATE: localid 9, mac 00:06:25:09:39:5d,
flags 0000012fh, to change state to KILLING
Localid 9, globalid SESSION-9-893249336 moved from ACTIVE to KILLING
(client=00:06:25:09:39:5d)
```

Managing System Files

About System Files 517
Working with Files 520
Managing Configuration Files 526
Backing Up and Restoring the System 532
Upgrading the System Image 535

A WLAN—Security Switch (WSS) contains nonvolatile storage. WSS Software allows you to manage the files in nonvolatile storage. In addition, you can copy files between the WSS and a TFTP server on the network.

About System Files

Generally, an WSS switch's nonvolatile storage contains the following types of files:

- System image files—The operating system software for the WSS switch and its attached AP access ports
- Configuration files—CLI commands that configure the WSS and its attached AP access ports
- System log files—Files containing log entries generated by WSS Software.

When you power on or reset the WSS or reboot the software, the switch loads a designated system image, then loads configuration information from a designated configuration file.

An WSS switch can also contain temporary files with trace information used for troubleshooting. Temporary files are not stored in nonvolatile memory, but are listed when you display a directory of the files on the switch.

Displaying Software Version Information

To display the software, firmware, and hardware versions, use the following command:

show version [details]

The **details** option displays hardware and software information about the AP access ports configured on the WSS switch.

To display version information for an WSS switch, type the following command:

23x0# show version

```
        Mobility System Software, Version: 3.0.0
        Copyright (c) 2003,2004 by Nortel , Inc

Build Information: (build#75) TOP 2004-06-30 07:25:00
Model:             WSS-20
Hardware
   Mainboard:      version 0 ; FPGA version 0
   PoE board:      version 1 ; FPGA version 6
Serial number      0321300013
Flash:             3.0.0.375  - md0a
Kernel:            3.0.0#43: Wed Jun 30 05:17:44 PDT 2004
BootLoader:        1.19 / 1.7.4
```

To also display AP access point information, type the following command:

23x0# show version details

```
        Mobility System Software, Version: 3.0.0
        Copyright (c) 2003,2004 by Nortel , Inc

Build Information: (build#75) TOP 2004-06-30 07:25:00
Model:             WSS-20
Hardware
   Mainboard:      version 0 ; FPGA version 0
   PoE board:      version 1 ; FPGA version 6
Serial number      0321300013
Flash:             3.0.0.375  - md0a
Kernel:            3.0.0#43: Wed Jun 30 05:17:44 PDT 2004
BootLoader:        1.19 / 1.7.4

Port/DAP AP Model   Serial #    Versions
-------- ---------- ----------- ------------------------
-   /23  AP-252     0123456789  H/W  : A3
                                F/W1 : 5.6
                                F/W2 : 5.6
                                S/W  : 3.0.0
-   /24  AP-241     9876543210  H/W  : A3
                                F/W1 : 5.6
```

```
F/W2 : N/A
S/W  : 3.0.0
```

(For additional information about the output, see the *Nortel Mobility System Software Command Reference*.)

Displaying Boot Information

Boot information consists of the WSS Software version and the names of the system image file and configuration file currently running on the WSS switch. The **boot** command also lists the system image and configuration file that will be loaded after the next reboot. The currently running versions are listed in the Booted fields. The versions that will be used after the next reboot are listed in the Configured fields.

To display boot information, type the following command:

```
23x0# show boot
Configured boot image:           boot0:WSS020003.020
Configured boot configuration:   file:newconfig
Booted version:                  2.0.3
Booted image:                    boot1:WSS020101.020
Booted configuration:            file:configuration
Product model:                   WSS-20
```

In this example, the switch is running software version 1.1.0. The switch used the *WSS010100.020* image file in boot partition boot1 and the *configuration* configuration file for the most recent reboot. The switch is set to use image file *WSS010101.020* in boot partition boot0 and configuration file *newconfig* for the next reboot.

(For additional information about the output, see the *Nortel Mobility System Software Command Reference*.)

Working with Files

The following section describe how to manage files stored on the WSS switch.

Displaying a List of Files

Files are stored on an WSS switch in the following areas:

- File—Contains configuration files
- Boot—Contains system image files
- Temporary—Contains log files and other files created by WSS Software

The file and boot areas are in nonvolatile storage. Files in nonvolatile storage remain in storage following a software reload or power cycle. The files in the temporary area are removed following a software reload or power cycle.

The boot area is divided into two partitions, boot0 and boot1. Each partition can contain one system image file.

The file area can contain subdirectories. Subdirectory names are indicated by a forward slash at the end of the name. In the following example, *dangdir* and *old* are subdirectories.

To display a list of the files in nonvolatile storage and temporary files, type the following command:

23x0# **dir**

```
==========================================================================
file:
Filename                                        Size           Created
file:configuration                             17 KB     May 21 2004, 18:20:53
file:configuration.txt                        379 bytes  May 09 2004, 18:55:17
file:dangcfg                                   13 KB     May 16 2004, 18:30:44
dangdir/                                      512 bytes  May 16 2004, 17:23:44
old/                                          512 bytes  Sep 23 2003, 21:58:48
Total:          32 Kbytes used, 207824 Kbytes free
==========================================================================
Boot:
Filename                                        Size           Created
*boot0:bload                                  746 KB     May 09 2004, 19:02:16
*boot0:WSS030000.020                         8182 KB     May 09 2004, 18:58:16
boot1:WSS030000.020                          8197 KB     May 21 2004, 18:01:02
Boot0: Total:        8928 Kbytes used, 3312 Kbytes free
Boot1: Total:        8197 Kbytes used, 4060 Kbytes free
==========================================================================
temporary files:
Filename                                        Size           Created
Total:         0 bytes used, 93537 Kbytes free
Total:  15 Kbytes used, 90941 Kbytes free
```

The following command displays the files in the *old* subdirectory:

23x0# **dir old**

```
==========================================================================
file:
Filename                                        Size           Created
file:configuration.txt                      3541 bytes   Sep 22 2003, 22:55:44
file:configuration.xml                        24 KB      Sep 22 2003, 22:55:44
Total:          27 Kbytes used, 207824 Kbytes free
```

(For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*)

Copying a File

You can perform the following copy operations:

- Copy a file from a TFTP server to nonvolatile storage.
- Copy a file from nonvolatile storage or temporary storage to a TFTP server.
- Copy a file from one area in nonvolatile storage to another.
- Copy a file to a new filename in nonvolatile storage.

To copy a file, use the following command.

copy *source-url destination-url*

A URL can be one of the following:

- [*subdirname*/]*filename*
- **file:**[*subdirname*/]*filename*
- **tftp:**//*ip-addr*/[*subdirname*/]*filename*
- **tmp:***filename*

The *filename* and **file:***filename* URLs are equivalent. You can use either URL to refer to a file in an WSS switch's nonvolatile memory.

The **tftp://***ip-addr*/*filename* URL refers to a file on a TFTP server. If DNS is configured on the WSS switch, you can specify a TFTP server's hostname as an alternative to specifying the IP address.

The **tmp:***filename* URL refers to a file in temporary storage. You can copy a file out of temporary storage but you cannot copy a file into temporary storage.

The *subdirname/* option specifies a subdirectory.

If you are copying a system image file into nonvolatile storage, the *destination-url* must include the boot partition name. You can specify one of the following:

- **boot0:/***filename*
- **boot1:/***filename*

You must specify the boot partition that *was not* used to load the currently running image.



Note. You can copy a file from an WSS switch to a TFTP server or from a TFTP server to an WSS switch, but you cannot use WSS Software to copy a file directly from one TFTP server to another.

To copy the file *floor2WSS* from nonvolatile storage to a TFTP server, type the following command:

```
23x0# copy floor2WSS tftp://10.1.1.1/floor2WSS
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
```

The above command copies the file to the same filename on the TFTP server. To rename the file when copying it, type the following command:

```
23x0# copy floor2WSS tftp://10.1.1.1/floor2WSS-backup
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
```

To copy a file named *newconfig* from a TFTP server to nonvolatile storage, type the following command:

```
23x0# copy tftp://10.1.1.1/newconfig newconfig
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

The above command copies the file to the same filename. To rename the file when copying it, type the following command:

```
23x0# copy tftp://10.1.1.1/newconfig WSSconfig
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

To copy system image *WSS010101.020* from a TFTP server to boot partition 1 in nonvolatile storage, type the following command:

```
23x0# copy tftp://10.1.1.107/WSS010101.020 boot1:WSS010101.020
.................................................................................
.............................success: received 8163214 bytes in 105.939 seconds
[ 86495 bytes/sec]
```

To rename *test-config* to *new-config*, you can copy it from one name to the other in the same location, and then delete *test-config*. Type the following commands:

```
23x0# copy test-config new-config

23x0# delete test-config
success: file deleted.
```

To copy file *corpa-login.html* from a TFTP server into subdirectory *corpa* in an WSS switch's nonvolatile storage, type the following command:

```
23x0# copy tftp://10.1.1.1/corpa-login.html corpa/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

Deleting a File

Warning! WSS Software does not prompt you to verify whether you want to delete a file. When you press Enter after typing a **delete** command, WSS Software immediately deletes the specified file. Nortel recommends that you copy a file to a TFTP server before deleting the file.

Note. WSS Software does not allow you to delete the currently running software image file or the running configuration.

To delete a file, use the following command:

delete *url*

The URL can be a filename of up to 128 alphanumeric characters.

To copy a file named *testconfig* to a TFTP server and delete the file from nonvolatile storage, type the following commands:

```
23x0# copy testconfig tftp://10.1.1.1/testconfig
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
23x0# delete testconfig
success: file deleted.
```

Creating a Subdirectory

You can create subdirectories in the user files area of nonvolatile storage. To create a subdirectory, use the following command:

mkdir [*subdirname*]

To create a subdirectory called *corp2* and display the root directory to verify the result, type the following commands:

23x0# **mkdir corp2**
```
success: change accepted.
```

23x0# **dir**
```
================================================================================
file:
Filename                                        Size           Created
file:configuration                               17 KB      May 21 2004, 18:20:53
file:configuration.txt                          379 bytes   May 09 2004, 18:55:17
corp2/                                          512 bytes   May 21 2004, 19:22:09
corp_a/                                         512 bytes   May 21 2004, 19:15:48
file:dangcfg                                     13 KB      May 16 2004, 18:30:44
dangdir/                                        512 bytes   May 16 2004, 17:23:44
old/                                            512 bytes   Sep 23 2003, 21:58:48
Total:          33 Kbytes used, 207822 Kbytes free
================================================================================
Boot:
Filename                                        Size           Created
*boot0:bload                                    746 KB      May 09 2004, 19:02:16
*boot0:WSS030000.020                           8182 KB      May 09 2004, 18:58:16
boot1:WSS030000.020                            8197 KB      May 21 2004, 18:01:02
Boot0: Total:        8928 Kbytes used, 3312 Kbytes free
Boot1: Total:        8197 Kbytes used, 4060 Kbytes free
================================================================================
temporary files:
Filename                                        Size           Created
Total:         0 bytes used, 93537 Kbytes free
```

Removing a Subdirectory

To remove a subdirectory from nonvolatile storage, use the following command:

rmdir [*subdirname*]

To remove subdirectory *corp2*, type the following example:

```
23x0# rmdir corp2
success: change accepted.
```

Managing Configuration Files

A configuration file contains CLI commands that set up the WSS switch. The switch loads a designated configuration file immediately after loading the system software when the software is rebooted. You also can load a configuration file while the switch is running to change the switch's configuration.

When you enter CLI commands to make configuration changes, these changes are immediately added to the device's running configuration but are not saved to the configuration file.

This section describes how to display the running configuration and the configuration file, and how to save and load configuration changes. A procedure is also provided for resetting the WSS switch to its factory default configuration.

Displaying the Running Configuration

To display the configuration running on the WSS switch, use the following command:

show config [area *area***] [all]**

The **area** *area* parameter limits the display to a specific configuration area. (For more information, see the *Nortel Mobility System Software Command Reference*.)

The **all** parameter includes all commands that are set at their default values. Without the **all** parameter, the **show config** command lists only those configuration commands that set a parameter to a value other than the default.

To display the running configuration, type the following command:

```
23x0# show config
# Configuration nvgen'd at 2004-5-10 19:08:38
# Image 2.1.0
# Model WSS-20
# Last change occurred at 2004-5-10 16:31:14
set trace authentication level 10
set ip dns server 10.10.10.69 PRIMARY
set ip dns server 10.20.10.69 SECONDARY
set ip route default 10.8.1.1 1
set log console disable severity debug
set log session disable severity alert
set log buffer enable severity error messages 200
set log trace disable severity error mbytes 10
set log server 192.168.253.11 severity critical
set timezone PST -8 0
set summertime PDT start first sun apr 2 0 end last sun oct 2 0
set system name WSS-20
set system countrycode US
set system contact nortel-pubs
set radius server r1 address 192.168.253.1 key sunflower
set server group sg1 members r1
set enablepass password b6b706525e1814394621eeb2a1c4d5803fcf
set authentication console * none
set authentication admin * none
set user tech password encrypted 1315021018
press any key to continue, q to quit.
```

To display only the VLAN configuration commands, type the following command:

```
23x0# show config area vlan
# Configuration nvgen'd at 2004-5-10 19:08:38
# Image 2.1.0
# Model WSS-20
# Last change occurred at 2004-5-10 16:31:14
set vlan 1 port 1
set vlan 10 name backbone tunnel-affinity 5
set vlan 10 port 21
```

```
set vlan 10 port 22
set vlan 3 name red tunnel-affinity 5
set igmp mrsol mrsi 60 vlan 1
set igmp mrsol mrsi 60 vlan 10
```

Saving Configuration Changes

To save the running configuration to a configuration file, use the following command:

save config [*filename*]

If you do not specify a filename of up to 128 alphanumeric characters, the command replaces the startup configuration file that was loaded the last time the software was rebooted. (To display the filename of that configuration file, see "Displaying Boot Information" on page 520.)

To save the running configuration to the file loaded the last time the software was rebooted, type the following command:

```
23x0# save config
success: configuration saved.
```

To save the running configuration to a file named *newconfig*, type the following command:

```
23x0# save config newconfig
success: configuration saved to newconfig.
```

Specifying the Configuration File to Use After the Next Reboot

By default, the WSS switch loads the configuration file named *configuration* from nonvolatile storage following a software reboot. To use a different configuration file in nonvolatile storage after rebooting, use the following command:

set boot configuration-file *filename*

To configure an WSS switch to load the configuration file *floor2WSS* from nonvolatile storage following the next software reboot, type the following command:

```
23x0# set boot configuration-file floor2WSS
success: boot config set.
```

Loading a Configuration File



Caution! This command completely removes the running configuration and replaces it with the configuration contained in the file. Nortel recommends that you save a copy of the current running configuration to a backup configuration file before loading a new configuration.

To load configuration commands from a file into the WSS's running configuration, use the following command:

load config [*url*]

The default URL is the name of the configuration file loaded after the last reboot.

To load a configuration file named *newconfig*, type the following command:

```
23x0# load config newconfig
Reloading configuration may result in lost of connectivity, do you wish to
continue? (y/n) [n]y
success: Configuration reloaded
```

After you type **y**, WSS Software replaces the running configuration with the configuration in the *newconfig* file. If you type **n**, WSS Software does not load the *newconfig* file and the running configuration remains unchanged.

Resetting to the Factory Default Configuration

To reset the WSS switch to its factory default configuration, use the following command:

clear boot config

This command removes the configuration file that the WSS switch searches for after the software is rebooted.

To back up the current configuration file named *configuration* and reset the WSS switch to the factory default configuration, type the following commands:

```
23x0# copy configuration tftp://10.1.1.1/backupcfg
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]

23x0# clear boot config
success: Reset boot config to factory defaults.

23x0# reset system force
...... rebooting ......
```

The **reset system force** command reboots the switch. The **force** option immediately restarts the system and reboots. If you do not use the **force** option, the command first compares the running configuration to the configuration file. If the files do not match, WSS Software does not restart the WSS switch but instead displays a message advising you to either save the configuration changes or use the **force** option.

Backing Up and Restoring the System

WSS Software has commands that enable you to easily backup and restore WSS system and user files:

backup system [**tftp:**/*ip-addr*/]*filename* [**all** | **critical**]

restore system [**tftp:**/*ip-addr*/]*filename* [**all** | **critical**] [**force**]

The **backup** command creates an archive in Unix *tape archive* (*tar*) format.

The **restore** command unzips an archive created by the **backup** command and copies the files from the archive onto the switch. If a file in the archive has a counterpart on the switch, the archive version of the file replaces the file on the switch. The **restore** command does not delete files that do not have counterparts in the archive. For example, the command does not completely replace the user files area. Instead, files in the archive are added to the user files area. A file in the user area is replaced only if the archive contains a file with the same name.

You can create or unzip an archive located on a TFTP server or in the switch's nonvolatile storage. If you specify a TFTP server as part of the filename with the **backup** command, the archive is copied directly to the TFTP server and not stored locally on the switch.

Both commands have options to specify the types of files you want to back up and restore:

- **critical**—Backs up or restores system files, including the configuration file used when booting, and certificate files. The size of an archive created by this option is generally 1MB or less. This is the default for the **restore** command.
- **all**—Backs up or restores the same files as the **critical** option, ***and*** all files in the user files area of nonvolatile storage. (The user files area contains the set of files listed in the *file* section of **dir** command output.) Archive files created by the **all** option are larger than files created by the **critical** option. The file size depends on the files in the

user area, and the file can be quite large if the user area contains image files. This is the default for the **backup** command.



Note. If the archive's files cannot fit on the switch, the restore operation fails. Nortel recommends deleting unneeded image files before creating or restoring an archive.

Use the **critical** option if you want to back up or restore only the system-critical files required to operate and communicate with the switch. Use the **all** option if you also want to back up or restore Web-based AAA pages, backup configuration files, image files, and any other files stored in the user files area of nonvolatile storage.

Neither option archives image files or any other files listed in the *Boot* section of **dir** command output. The **all** option archives image files only if they are present in the user files area.

The **backup** command stores the MAC address of the switch in the archive. By default, the **restore** command works only if the MAC address in the archive matches the MAC address of the switch where the **restore** command is entered. The **force** option overrides this restriction and allows you to unpack one switch's archive onto another switch.



Caution! Do not use the **force** option unless advised to do so by Nortel NETS. If you restore one switch's system files onto another switch, you must generate new key pairs and certificates on the switch.

Managing Configuration Changes

The **backup** command places the boot configuration file into the archive. (The boot configuration file is the *Configured boot configuration* in the **show boot** command's output.) If the running configuration contains changes that have not been saved, these changes are not in the boot configuration file and are not archived. To make sure the archive contains the configuration that is currently running on the switch, use the **save config** command to save the running configuration to the boot configuration file, before using the **backup** command.

The **restore** command replaces the boot configuration on the switch with the one in the archive. The boot configuration includes the configuration filename and the image filename to use after the next switch restart. (These are the *Configured boot image* and *Configured boot configuration* files listed in the **show boot** command's output.) The **restore** command does not affect the running image or the running configuration.

If you want to use the configuration in the boot configuration file restored from an archive instead of the configuration currently running on the switch, use the **load config** command to load the boot configuration file, or restart the switch. If instead, you want to replace the configuration restored from the archive with the running configuration, use the **save config** command to save the running configuration to the boot configuration file.



Note. The next time the switch is restarted after the **restore** command is used, the switch uses the boot configuration filename that was in use when the archive was created. If you change the boot configuration filename after creating the archive, the new name is not used when the switch is restarted. To use the new configuration, use the **save config** *filename* command, where *filename* is the name of the boot configuration file restored from the archive, before you restart the switch. If you have already restarted the switch, use the **load config** *filename* command to load the new configuration, then use the **save config** *filename* command.

Backup and Restore Examples

The following command creates an archive of the system-critical files and copies the archive directly to a TFTP server. The filename in this example includes a TFTP server IP address, so the archive is not stored locally on the switch.

```
23x0# backup system tftp:/10.10.20.9/sysa_bak critical

success: sent 28263 bytes in 0.324 seconds [ 87231 bytes/sec]
```

The following command restores system-critical files on a switch, from archive *sysa_bak*:

```
23x0# restore system tftp:/10.10.20.9/sysa_bak
success: received 11908 bytes in 0.150 seconds [ 79386 bytes/sec]

success: restore complete.
```

Upgrading the System Image

See the release notes for upgrade information.

Rogue Detection and Countermeasures

About Rogues and RF Detection 537
Summary of Rogue Detection Features 542
Configuring Rogue Detection Lists 543
Enabling Countermeasures 548
Disabling or Reenabling Active Scan 549
Enabling AP Signatures 549
Disabling or Reenabling Logging of Rogues 550
Enabling Rogue and Countermeasures Notifications 550
IDS and DoS Alerts 550
Displaying RF Detection Information 561

AP radios automatically scan the RF spectrum for other devices transmitting in the same spectrum. The RF scans discover third-party transmitters in addition to other Nortel radios. WSS Software considers the non-Nortel transmitters to be *devices of interest*, which are potential rogues.

You can display information about the devices of interest. To identify friendly devices, such as non-Nortel access ports in your network or neighbor's network, you can add them to the known devices list. You also can enable countermeasures to prevent clients from using the devices that truly are rogues.

With WLAN Management Software , you also can display the physical location of a rogue device. (For more information, see the *Nortel WLAN Management Software Reference Manual*.)

About Rogues and RF Detection

RF detection detects all the IEEE 802.11 devices in a Mobility Domain and can single out the unauthorized rogue access points.

Rogue access points and Clients

A rogue access point is an access point that is not authorized to operate in a network. Rogue access points and their clients undermine the security of an enterprise network by potentially allowing unchallenged access to the network by any wireless user or client in the physical vicinity. Rogue access points and users can also interfere with the operation of your enterprise network.

Rogue Classification

When WSS Software detects a third-party wireless device that is not allowed on the network, WSS Software classifies the device as one of the following:

- Rogue—The device is in the Nortel network but does not belong there.
- Interfering device—The device is not part of the Nortel network but also is not a rogue. No client connected to the device has been detected communicating with any network entity listed in the forwarding database (FDD) of any WSS switch in the Mobility Domain. Although the interfering device is not connected to your network, the device might be causing RF interference with AP radios.

When you enable countermeasures, you can specify whether to issue them against rogues and interfering devices, or against rogues only. For example, if you do not want to issue countermeasures against your neighbor's wireless devices, you can select to issue countermeasures against rogues only. RF Auto-Tuning can automatically change AP radio channels to work around interfering devices without attacking those devices.

Rogue Detection Lists

Rogue detection lists specify the third-party devices and SSIDs that WSS Software allows on the network, and the devices WSS Software classifies as rogues. You can configure the following rogue detection lists:

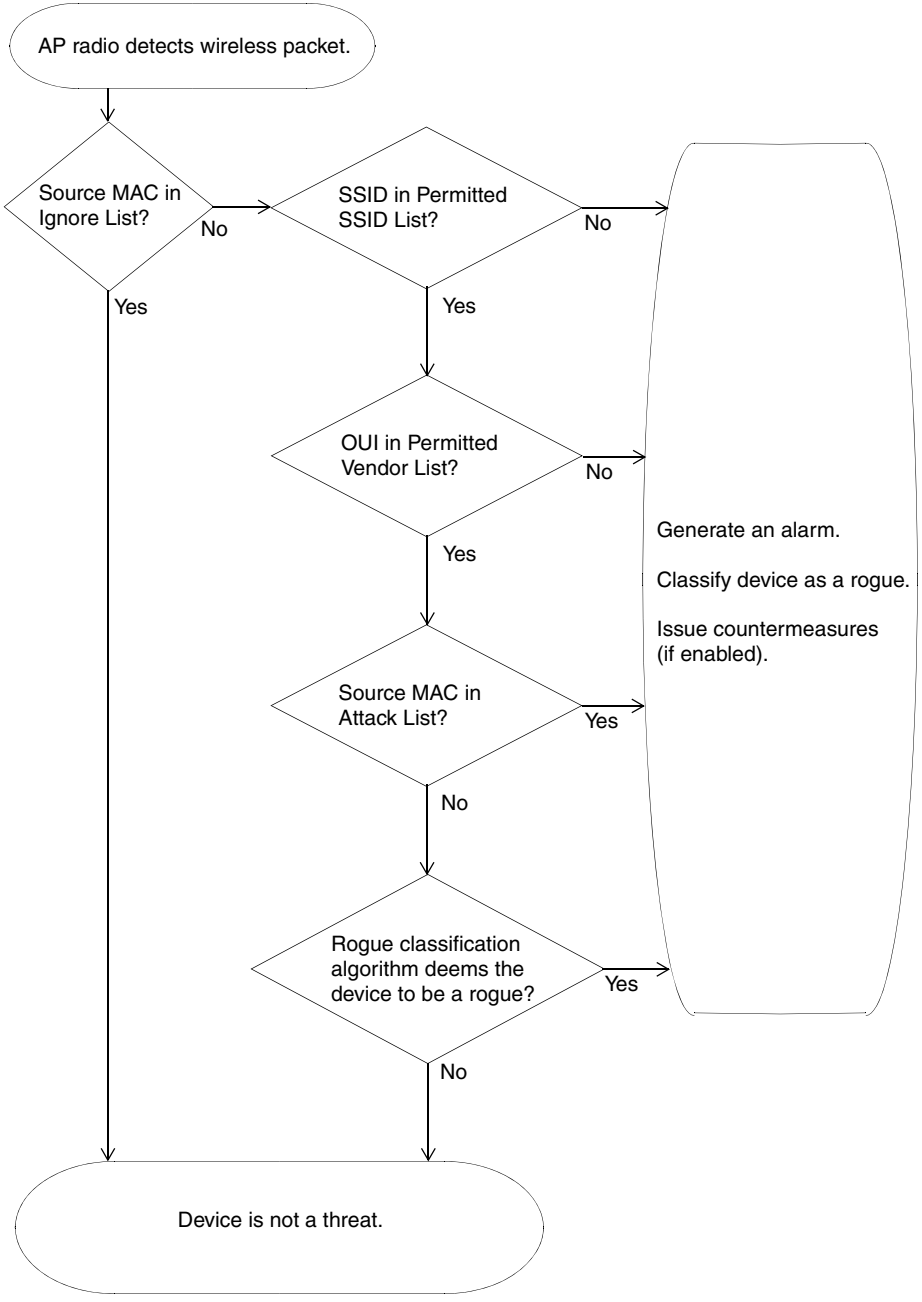
- Permitted SSID list—A list of SSIDs allowed in the Mobility Domain. WSS Software generates a message if an SSID that is not on the list is detected.
- Permitted vendor list—A list of the wireless networking equipment vendors whose equipment is allowed on the network. The vendor of a piece of equipment is identified by the Organizationally Unique Identifier (OUI), which is the first three bytes of the equipment's MAC address. WSS Software generates a message if an AP or wireless client with an OUI that is not on the list is detected.
- Client black list—A list of MAC addresses of wireless clients who are not allowed on the network. WSS Software prevents clients on the list from accessing the network through an WSS switch. If the client is placed on the black list dynamically by WSS Software due to an association, reassociation or disassociation flood, WSS Software generates a log message.
- Ignore list—A list of third-party devices that you want to exempt from rogue detection. WSS Software does not count devices on the ignore list as rogues or interfering devices, and does not issue countermeasures against them.

An empty permitted SSID list or permitted vendor list implicitly allows all SSIDs or vendors. However, when you add an entry to the SSID or vendor list, all SSIDs or vendors that are not in the list are implicitly disallowed. An empty client black list implicitly allows all clients, and an empty ignore list implicitly considers all third-party wireless devices to be potential rogues.

All the lists except the black list require manual configuration. You can configure entries in the black list and WSS Software also can place a client in the black list due to an association, reassociation or disassociation flood from the client.

The rogue classification algorithm examines each of these lists when determining whether a device is a rogue. Figure 21 on page 540 shows how the rogue detection algorithm uses the lists.

Figure 21: Rogue Detection Algorithm



RF Detection Scans

All radios continually scan for other RF transmitters. Radios perform passive scans and active scans:

- Passive scans—The radio listens for beacons and probe responses.
- Active scans—The radio sends *probe any* requests (probe requests with a null SSID name) to solicit probe responses from other access ports.

Passive scans are always enabled and cannot be disabled. Active scans are enabled by default but can be disabled on a radio-profile basis.

Radios perform both types of scans on all channels allowed for the country of operation. (This is the regulatory domain set by the **set system countrycode** command.) 802.11b/g radios scan in the 2.4 GHz to 2.4835 GHz spectrum. 802.11a radios scan in the 5.15 GHz to 5.85 GHz spectrum.

Both enabled radios and disabled radios perform these scans.

Dynamic Frequency Selection (DFS)

Some regulatory domains require conformance to ETSI document EN 301 893. Section 4.6 of that document specifies requirements for Dynamic Frequency Selection (DFS). These requirements apply to radios operating in the 5 GHz band (802.11a radios).

In countries where Dynamic Frequency Selection (DFS) is required, WSS Software performs the appropriate check for radar. If radar is detected on a channel, the AP radio stops performing active scans on that channel in accordance with DFS. However, the radio continues to passively scan for beacons from rogue devices.

When an AP radio detects radar on a channel, the radio switches to another channel and does not attempt to use the channel where the radar was detected for 30 minutes. WSS Software also generates a message.



Note. The Auto-RF feature must be enabled. Otherwise WSS Software cannot change the channel.

Countermeasures

You can enable WSS Software to use countermeasures against rogues. Countermeasures consist of packets that interfere with a client's ability to use the rogue.

Countermeasures are disabled by default. You can enable them on an individual radio-profile basis. When you enable them, all devices of interest that are not in the known devices list become viable targets for countermeasures. The Mobility Domain's seed switch automatically selects individual radios to send the countermeasure packets.

Summary of Rogue Detection Features

Table 33 lists the rogue detection features in WSS Software.

Table 33: Rogue Detection Features

Rogue Detection Feature	Description	Applies To	
		Third-Party APs	Clients
Classification	WSS Software can classify third-party APs as rogues or interfering devices. A rogue is a third-party AP whose MAC address WSS Software knows. An interfering device does not have a MAC address known to WSS Software. WSS Software can detect rogue clients, locate their APs, and issue countermeasures against the APs.	Yes	Yes
Permitted vendor list	List of OUIs to allow on the network. An OUI is the first three octets of a MAC address and uniquely identifies an AP's or client's vendor.	Yes	No
Permitted SSID list	List of SSIDs allowed on the network. WSS Software can issue countermeasures against third-party APs sending traffic for an SSID that is not on the list.	Yes	No
Client black list	List of client MAC addresses that are not allowed on the wireless network. WSS Software drops all packets from these clients.	No	Yes
Attack list	List of AP MAC addresses to attack. WSS Software can issue countermeasures against these APs whenever they are detected on the network.	Yes	No

Table 33: Rogue Detection Features (continued)

Rogue Detection Feature	Description	Applies To	
		Third-Party APs	Clients
Ignore list	List of MAC addresses to ignore during RF detection. WSS Software does not classify devices on this list as rogues or interfering devices, and does not issue countermeasures against them.	Yes	Yes
Countermeasures	Packets sent by Nortel APs to interfere with the operation of a rogue. Countermeasures are configurable a radio-profile basis.	Yes	Yes
Active scan	Active scan sends probe any requests (probes with a null SSID name) to look for rogue APs. Active scan is configurable on a radio-profile basis.	Yes	No
Nortel AP signature	Value in an AP's management frames that identifies the AP to WSS Software. AP signatures help prevent spoofing of the AP MAC address.	No	No
Log messages and traps	Messages and traps for rogue activity. Messages are described in "IDS and DoS Alerts" on page 550.	Yes	Yes

Configuring Rogue Detection Lists

The following sections describe how to configure lists to specify the devices that are allowed on the network and the devices that WSS Software should attack with countermeasures.

(For information about how WSS Software uses the lists, see "Rogue Detection Lists" on page 538.)

Configuring a Permitted Vendor List

The permitted vendor list specifies the third-party AP or client vendors that are allowed on the network. WSS Software does not list a device as a rogue or interfering device if the device's OUI is in the permitted vendor list.

By default, the permitted vendor list is empty and all vendors are allowed. If you configure a permitted vendor list, WSS Software allows only the devices whose OUIs are on the list. The permitted vendor list applies only to the WSS switch on which the list is configured. WSS switches do not share permitted vendor lists.

To add an entry to the permitted vendor list, use the following command:

set rfdetect vendor-list {client | ap} *mac-addr*

The following command adds an entry for clients whose MAC addresses start with aa:bb:cc:

```
23x0# set rfdetect vendor-list client aa:bb:cc:00:00:00
success:  MAC aa:bb:cc:00:00:00 is now in client vendor-list.
```

The trailing 00:00:00 value is required.

To display the permitted vendor list, use the following command:

show rfdetect vendor-list

The following example shows the permitted vendor list on WSS switch:

```
23x0# show rfdetect vendor-list
Total number of entries: 1
       OUI         Type
----------------- ------
aa:bb:cc:00:00:00 client
11:22:33:00:00:00 ap
```

To remove an entry from the permitted vendor list, use the following command:

clear rfdetect vendor-list {client | ap} {*mac-addr* **| all}**

The following command removes client OUI aa:bb:cc:00:00:00 from the permitted vendor list:

```
23x0# clear rfdetect vendor-list client aa:bb:cc:00:00:00
success: aa:bb:cc:00:00:00 is no longer in client vendor-list.
```

Configuring a Permitted SSID List

The permitted SSID list specifies the SSIDs that are allowed on the network. If WSS Software detects packets for an SSID that is not on the list, the AP that sent the packets is classified as a rogue. WSS Software issues countermeasures against the rogue if they are enabled.

By default, the permitted SSID list is empty and all SSIDs are allowed. If you configure a permitted SSID list, WSS Software allows traffic only for the SSIDs that are on the list. The permitted SSID list applies only to the WSS switch on which the list is configured. WSS switches do not share permitted SSID lists.

To add an SSID to the list, use the following command:

set rfdetect ssid-list *ssid-name*

The following command adds SSID *mycorp* to the list of permitted SSIDs:

```
23x0# set rfdetect ssid-list mycorp
success:  ssid mycorp is now in ssid-list.
```

To display the permitted SSID list, use the following command:

show rfdetect ssid-list

The following example shows the permitted SSID list on WSS switch:

```
23x0# show rfdetect ssid-list
Total number of entries: 3
       SSID
-----------------
           mycorp
        corporate
            guest
```

To remove an SSID from the permitted SSID list, use the following command:

clear rfdetect ssid-list *ssid-name*

The following command clears SSID *mycorp* from the permitted SSID list:

```
23x0# clear rfdetect ssid-list mycorp
success: mycorp is no longer in ssid-list.
```

Configuring a Client Black List

The client black list specifies clients that are not allowed on the network. WSS Software drops all packets from the clients on the black list.

By default, the client black list is empty. In addition to manually configured entries, the list can contain entries added by WSS Software. WSS Software can place a client in the black list due to an association, reassociation or disassociation flood from the client.

The client black list applies only to the WSS switch on which the list is configured. WSS switches do not share client black lists.

To add an entry to the list, use the following command:

set rfdetect black-list *mac-addr*

The following command adds client MAC address 11:22:33:44:55:66 to the black list:

```
23x0# set rfdetect black-list 11:22:33:44:55:66
success:  MAC 11:22:33:44:55:66 is now blacklisted.
```

To display the client black list, use the following command:

show rfdetect black-list

The following example shows the client black list on WSS switch:

```
23x0# show rfdetect black-list
Total number of entries: 1
  Blacklist MAC         Type          Port   TTL
----------------- ----------------- ------- ---
11:22:33:44:55:66 configured        -         -
11:23:34:45:56:67 assoc req flood   3        25
```

To remove a MAC address from the client black list, use the following command:

clear rfdetect black-list *mac-addr*

The following command removes MAC address 11:22:33:44:55:66 from the black list:

```
23x0# clear rfdetect black-list 11:22:33:44:55:66
success: 11:22:33:44:55:66 is no longer blacklisted.
```

Configuring an Attack List

The attack list specifies the MAC address of devices that WSS Software should issue countermeasures against whenever the devices are detected on the network. The attack list can contain the MAC addresses of APs and clients.

By default, the attack list is empty. The attack list applies only to the WSS switch on which the list is configured. WSS switches do not share attack lists.

To add an entry to the list, use the following command:

set rfdetect attack-list *mac-addr*

The following command adds MAC address aa:bb:cc:44:55:66 to the attack list:

```
23x0# set rfdetect attack-list 11:22:33:44:55:66
success:  MAC 11:22:33:44:55:66 is now in attacklist.
```

To display the attack list, use the following command:

show rfdetect attack-list

The following example shows the attack list on WSS switch:

```
23x0# show rfdetect attack-list
Total number of entries: 1
 Attacklist MAC    Port/Radio/Chan   RSSI      SSID
----------------- ----------------- ------ ------------
11:22:33:44:55:66  dap 2/1/11       -53    rogue-ssid
```

To remove a MAC address from the attack list, use the following command:

clear rfdetect attack-list *mac-addr*

The following command clears MAC address 11:22:33:44:55:66 from the attack list:

```
23x0# clear rfdetect attack-list 11:22:33:44:55:66
success: 11:22:33:44:55:66 is no longer in attacklist.
```

Configuring an Ignore List

By default, when countermeasures are enabled, WSS Software considers any non-Nortel transmitter to be a rogue device and can send countermeasures to prevent clients from using that device. To prevent WSS Software from sending countermeasures against a friendly device, add the device to the known devices list:

To add a device to the ignore list, use the following command:

set rfdetect ignore *mac-addr*

The *mac-addr* is the BSSID of the device you want to ignore.



Note. If you try to initiate countermeasures against a device on the ignore list, the ignore list takes precedence and WSS Software does not issue the countermeasures. Countermeasures apply only to rogue devices.

To ignore BSSID *aa:bb:cc:11:22:33* during all RF scans, type the following command:

```
2370# set rfdetect ignore aa:bb:cc:11:22:33
success:  MAC aa:bb:cc:11:22:33 is now ignored.
```

To remove a BSSID from the ignore list, use the following command:

clear rfdetect ignore *mac-addr*

To display the ignore list, use the following command:

show rfdetect ignore

The following command displays an ignore list containing two BSSIDs:

```
23x0# show rfdetect ignore
Total number of entries: 2
   Ignore MAC
-----------------
aa:bb:cc:11:22:33
aa:bb:cc:44:55:66
```

Enabling Countermeasures



Caution! Countermeasures affect wireless service on a radio. When an AP radio is sending countermeasures, the radio is disabled for use by network traffic, until the radio finishes sending the countermeasures.

Countermeasures are disabled by default. You can enable them on an individual radio profile basis. To enable countermeasures on a radio profile, use the following command:

set radio-profile *name* **countermeasures {all | rogue}**

The **all** option enables or disables countermeasures for rogues and for interfering devices. This option is equivalent to the scope of rogue detection in WSS Software Version 3.x. The **rogue** option enables or disables countermeasures for rogues only.

The following command enables countermeasures in radio profile *radprof3* for rogues only:

```
23x0# set radio-profile radprof3 countermeasures rogue
success: change accepted.
```

To disable countermeasures on a radio profile, use the following command:

clear radio-profile *name* **countermeasures**

The following command disables countermeasures in radio profile *radprof3*:

```
23x0# clear radio-profile radprof3 countermeasures
success: change accepted.
```

Disabling or Reenabling Active Scan

When active scanning is enabled, the AP radios managed by the switch look for rogue devices by sending *probe any* frames (probes with a null SSID name), to solicit probe responses from other APs.

Active scan is enabled by default. You can disable or reenable the feature on an individual radio profile basis. To disable or reenable active scan on a radio profile, use the following command:

set radio-profile *name* **active-scan {enable | disable}**

The following command disables active scan in radio profile *radprof3*:

```
23x0# set radio-profile radprof3 active-scan disable
success: change accepted.
```

Enabling AP Signatures

An AP signature is a set of bits in a management frame sent by an AP that identifies that AP to WSS Software. If someone attempts to spoof management packets from a Nortel AP, WSS Software can detect the spoof attempt.

AP signatures are disabled by default. To enable or disable them, use the following command:

set rfdetect signature {enable | disable}

The command applies only to APs managed by the WSS switch on which you enter the command. To enable signatures on all APs in a Mobility Domain, enter the command on each WSS switch in the Mobility Domain.



Note. You must use the same AP signature setting (enabled or disabled) on all WSS switches in a Mobility Domain.

Disabling or Reenabling Logging of Rogues

By default, an WSS switch generates a log message when a rogue is detected or disappears. To disable or reenable the log messages, use the following command:

set rfdetect log {enable | disable}

To display log messages on a switch, use the following command:

show log buffer

(This command has optional parameters. For complete syntax information, see the *Nortel Mobility System Software Command Reference*.)

Enabling Rogue and Countermeasures Notifications

By default, all SNMP notifications (informs or traps) are disabled. To enable or disable notifications for rogue detection, IDS, and DoS protection, configure a notification profile that sends all the notification types for these features. (For syntax information and an example, see "Configuring a Notification Profile" on page 162.)

IDS and DoS Alerts

WSS Software can detect illegitimate network access attempts and attempts to disrupt network service. In response, WSS Software generates messages and SNMP notifications. The following sections describe the types of attacks and security risks that WSS Software can detect.

For examples of the log messages that WSS Software generates when DoS attacks or other security risks are detected, see "IDS Log Message Examples" on page 559.

For information about the notifications, see "Configuring a Notification Profile" on page 162.



Note. To detect DoS attacks, active scan must be enabled. (See "Disabling or Reenabling Active Scan" on page 549.)

Flood Attacks

A flood attack is a type of Denial of Service attack. During a flood attack, a rogue wireless device attempts to overwhelm the resources of other wireless devices by continuously injecting management frames into the air. For example, a rogue client can repeatedly send association requests to try to overwhelm APs that receive the requests.

The threshold for triggering a flood message is 100 frames of the same type from the same MAC address, within a one-second period. If WSS Software detects more than 100 of the same type of wireless frame within one second, WSS Software generates a log message. The message indicates the frame type, the MAC address of the sender, the listener (AP and radio), channel number, and RSSI.

DoS Attacks

When active scan is enabled on APs, WSS Software can detect the following types of DoS attacks:

- RF Jamming—The goal of an RF jamming attack is to take down an entire WLAN by overwhelming the radio environment with high-power noise. A symptom of an RF jamming attack is excessive interference. If an AP radio detects excessive interference on a channel, and RF Auto-Tuning is enabled, WSS Software changes the radio to a different channel.
- Deauthenticate frames—Spoofed deauthenticate frames form the basis for most DoS attacks, and are the basis for other types of attacks including man-in-the-middle attacks. The source MAC address is spoofed so that clients think the packet is coming from a legitimate AP. If an AP detects a packet with its own source MAC address, the AP knows that the packet was spoofed.
- Broadcast deauthenticate frames—Similar to the spoofed deauthenticate frame attack above, a broadcast deauthenticate frame attack generates spoofed deauthenticate frames, with a broadcast destination address instead of the address of a specific client. The intent of the attack is to disconnect all stations attached to an AP.
- Disassociation frames—A disassociation frame from an AP instructs the client to end its association with the AP. The intent of this attack it to disconnect clients from the AP.
- Null probe responses—A client's probe request frame is answered by a probe response containing a null SSID. Some NIC cards lock up upon receiving such a probe response.
- Decrypt errors—An excessive number of decrypt errors can indicate that multiple clients are using the same MAC address. A device's MAC address is supposed to be unique. Multiple instances of the same address can indicate that a rogue device is pretending to be a legitimate device by spoofing its MAC address.
- Fake AP—A rogue device sends beacon frames for randomly generated SSIDs or BSSIDs. This type of attack can cause clients to become confused by the presence of so many SSIDs and BSSIDs, and thus interferes with the clients' ability to connect to valid APs. This type of attack can also interfere with RF Auto-Tuning when an AP is trying to adjust to its RF neighborhood.
- SSID masquerade—A rogue device pretends to be a legitimate AP by sending beacon frames for a valid SSID serviced by APs in your network. Data from clients that associate with the rogue device can be accessed by the hacker controlling the rogue device.
- Spoofed AP—A rogue device pretends to be a Nortel AP by sending packets with the source MAC address of the Nortel AP. Data from clients that associate with the rogue device can be accessed by the hacker controlling the rogue device.



Note. WSS Software detects a spoofed AP attack based on the fingerprint of the spoofed AP. Packets from the real AP have the correct signature, while spoofed packets lack the signature. (See "Enabling AP Signatures" on page 549.)

Netstumbler and Wellenreiter Applications

Netstumbler and Wellenreiter are widely available applications that hackers can use to gather information about the APs in your network, including location, manufacturer, and encryption settings.

Wireless Bridge

A wireless bridge can extend a wireless network outside the desired area. For example, someone can place a wireless bridge near an exterior wall to extend wireless coverage out into the parking lot, where a hacker could then gain access to the network.

Ad-Hoc Network

An ad-hoc network is established directly among wireless clients and does not use the infrastructure network (a network using an AP). An Ad-hoc network might not be an intentionally malicious attack on the network, but it does steal bandwidth from your infrastructure users.

Weak WEP Key Used by Client

A weak initialization vector (IV) makes a WEP key easier to hack. WSS Software alerts you regarding clients who are using weak WEP IVs so that you can strengthen the encryption on these clients or replace the clients.

Disallowed Devices or SSIDs

You can configure the following types of lists to explicitly allow specific devices or SSIDs:

- Permitted SSID list—WSS Software generates a message if an SSID that is not on the list is detected.
- Permitted vendor list—WSS Software generates a message if an AP or wireless client with an OUI that is not on the list is detected.
- Client black list—WSS Software prevents clients on the list from accessing the network through an WSS switch. If the client is placed on the black list dynamically by WSS Software due to an association, reassociation or disassociation flood, WSS Software generates a log message.

By default, these lists are empty and all SSIDs, vendors, and clients are allowed. For more information, see "Summary of Rogue Detection Features" on page 542.

Displaying Statistics Counters

To display IDS and DoS statistics counters, use the **show rfdetect counters** commands. (See “Displaying Statistics Counters” on page 558.)

IDS Log Message Examples

Table 34 shows examples of the log messages generated by IDS.

Table 34: IDS and DoS Log Messages

Message Type	Example Log Message
Probe message flood	Client aa:bb:cc:dd:ee:ff is sending probe message flood. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53.
Authentication message flood	Client aa:bb:cc:dd:ee:ff is sending authentication message flood. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53.
Null data message flood	Client aa:bb:cc:dd:ee:ff is sending null data message flood. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53.
Management frame 6 flood	Client aa:bb:cc:dd:ee:ff is sending rsvd mgmt frame 6 message flood. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53.
Management frame 7 flood	Client aa:bb:cc:dd:ee:ff is sending rsvd mgmt frame 7 message flood. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53.
Management frame D flood	Client aa:bb:cc:dd:ee:ff is sending rsvd mgmt frame D message flood. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53.
Management frame E flood	Client aa:bb:cc:dd:ee:ff is sending rsvd mgmt frame E message flood. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53.
Management frame F flood	Client aa:bb:cc:dd:ee:ff is sending rsvd mgmt frame F message flood. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53.
Associate request flood	Client aa:bb:cc:dd:ee:ff is sending associate request flood on port 2
Reassociate request flood	Client aa:bb:cc:dd:ee:ff is sending re-associate request flood on port 2
Disassociate request flood	Client aa:bb:cc:dd:ee:ff is sending disassociate request flood on port 2
Weak WEP initialization vector (IV)	Client aa:bb:cc:dd:ee:ff is using weak wep initialization vector. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53.
Decrypt errors	Client aa:bb:cc:dd:ee:ff is sending packets with decrypt errors. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53.
Spoofed deauthentication frames	Deauthentication frame from AP aa:bb:cc:dd:ee:ff is being spoofed. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53.
Spoofed disassociation frames	Disassociation frame from AP aa:bb:cc:dd:ee:ff is being spoofed. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53.
Null probe responses	AP aa:bb:cc:dd:ee:ff is sending null probe responses. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53.
Broadcast deauthentications	AP aa:bb:cc:dd:ee:ff is sending broadcast deauthentications. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53.

Table 34: IDS and DoS Log Messages (continued)

Message Type	Example Log Message
Fake AP SSID (when source MAC address is known)	FakeAP SSID attack detected from aa:bb:cc:dd:ee:ff. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53 SSID myssid.
Fake AP SSID (when source MAC address is not known)	FakeAP BSSID attack detected. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53 SSID myssid.
Spoofed SSID	AP Mac aa:bb:cc:dd:ee:ff(ssid myssid) is masquerading our ssid used by aa:bb:cc:dd:ee:fd. Detected by listener aa:bb:cc:dd:ee:fc(port 2, radio 1), channel 11 with RSSI -53.
Wireless bridge detected	Wireless bridge detected with address aa:bb:cc:dd:ee:ff. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53 SSID myssid.
Netstumbler detected	Netstumbler detected from aa:bb:cc:dd:ee:ff. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53 SSID myssid.
Wellenreiter detected	Wellenreiter detected from aa:bb:cc:dd:ee:ff. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53 SSID myssid.
Ad-hoc client frame detected	Adhoc client frame detected from aa:bb:cc:dd:ee:ff. Seen by AP on port 2, radio 1 on channel 11 with RSSI -53 SSID myssid.
Spoofed AP	AP Mac aa:bb:cc:dd:ee:ff(ssid myssid) is being spoofed. Received fingerprint 1122343 does not match our fingerprint 123344. Detected by listener aa:bb:cc:dd:ee:fd(port 2, radio 1), channel 11 with RSSI -53.
Disallowed SSID detected	AP Mac aa:bb:cc:dd:ee:ff(ssid myssid) is not part of ssid-list. Detected by listener aa:bb:cc:dd:ee:fd(port 2, radio 1), channel 11 with RSSI -53.
AP from disallowed vendor detected	AP Mac aa:bb:cc:dd:ee:ff(ssid myssid) is not part of vendor-list. Detected by listener aa:bb:cc:dd:ee:fd(port 2, radio 1), channel 11 with RSSI -53.
Client from disallowed vendor detected	Client Mac aa:bb:cc:dd:ee:ff is not part of vendor-list. Detected by listener aa:bb:cc:dd:ee:fd(port 2, radio 1), channel 11 with RSSI -53.
Interfering client seen on wired network	Client Mac aa:bb:cc:dd:ee:ff is seen on the wired network by WSS 10.1.1.1 on port 3 vlan 2 tag 1. Detected by listener aa:bb:cc:dd:ee:fd(port 2, radio 1), channel 11 with RSSI -53.

Displaying RF Detection Information

You can use the CLI commands listed in Table 35 to display rogue detection information.

Table 35: Rogue Detection Show Commands

Command	Description
show rfdetect clients [**mac** *mac-addr*]	Displays all wireless clients detected on the air.
show rfdetect counters	Displays statistics for rogue and Intrusion Detection System (IDS) activity detected by the APs managed by an WSS switch.
show rfdetect mobility-domain [**ssid** *ssid-name* | **bssid** *mac-addr*]	Displays information about rogues detected in a Mobility Domain. This command is valid only on the Mobility Domain's seed switch.
show rfdetect data	Displays information about all BSSIDs detected on the air, and labels those that are from rogues or interfering devices. This command is valid on any switch in the Mobility Domain.
show rfdetect visible *mac-addr* **show rfdetect visible ap** *AP-num* [**radio** {**1** | **2**}] **show rfdetect visible dap** *dap-num* [**radio** {**1** | **2**}]	Displays the BSSIDs detected by a specific Nortel radio.
show rfdetect countermeasures	Displays the current status of countermeasures against rogues in the Mobility Domain. This command is valid only on the Mobility Domain seed.
show rfdetect vendor-list	Displays the list of OUIs that are allowed on the network. An OUI identifies a piece of networking equipment's vendor. (See "Configuring a Permitted Vendor List" on page 544.)
show rfdetect ssid-list	Displays the list of SSIDs that are allowed on the network. (See "Configuring a Permitted SSID List" on page 545.)
show rfdetect black-list	Displays the list of wireless clients that are both allowed on the network. (See "Configuring a Client Black List" on page 546.)

Table 35: Rogue Detection Show Commands (continued)

Command	Description
show rfdetect attack-list	Displays the list of wireless devices that you want APs to attack with countermeasures. (See "Configuring an Attack List" on page 547.)
show rfdetect ignore	Displays the BSSIDs of third-party devices that WSS Software ignores during RF detection scans. (See "Configuring an Ignore List" on page 548.)

(For information about the fields in the output, see the *Nortel Mobility System Software Command Reference*.)

Displaying Rogue Clients

To display the wireless clients detected by an WSS switch, use the following command:

show rfdetect clients [**mac** *mac-addr*]

The following command shows information about all wireless clients detected by an WSS switch's APs:

```
23x0# show rfdetect clients
Total number of entries: 30
Client MAC        Client       AP MAC          AP     Port/Radio    NoL Type  Last
                  Vendor                     Vendor      /Channel            seen
----------------- ------- ----------------- ------- ------------- --- ----- ----

00:03:7f:bf:16:70 Unknown           Unknown           dap 1/1/6     1 intfr 207
00:04:23:77:e6:e5   Intel           Unknown           dap 1/1/2     1 intfr 155
00:05:5d:79:ce:0f  D-Link           Unknown           dap 1/1/149   1 intfr 87
00:05:5d:7e:96:a7  D-Link           Unknown           dap 1/1/149   1 intfr 117
00:05:5d:7e:96:ce  D-Link           Unknown           dap 1/1/157   1 intfr 162
00:05:5d:84:d1:c5  D-Link           Unknown           dap 1/1/1     1 intfr 52
```

The following command displays more details about a specific client:

```
23x0# show rfdetect clients mac 00:0c:41:63:fd:6d
Client Mac Address: 00:0c:41:63:fd:6d, Vendor: Linksys
   Port: dap 1, Radio: 1, Channel: 11, RSSI: -82, Rate: 2, Last Seen (secs ago): 84
    Bssid: 00:0b:0e:01:02:00, Vendor: Nortel, Type: intfr, Dst: ff:ff:ff:ff:ff:ff
     Last Rogue Status Check (secs ago): 3
```

The first line lists information for the client. The other lines list information about the most recent 802.11 packet detected from the client.

Displaying Rogue Detection Counters

To display rogue detection statistics counters, use the following command:

show rfdetect counters

The command shows counters for rogue activity detected by the WSS switch on which you enter the command.

```
23x0# show rfdetect counters
Type                                                Current      Total
--------------------------------------------------- ------------ ------------

Rogue access ports                                            0            0
Interfering access ports                                    139         1116
Rogue 802.11 clients                                          0            0
Interfering 802.11 clients                                    4          347
802.11 adhoc clients                                          0            1
Unknown 802.11 clients                                       20          965
Interfering 802.11 clients seen on wired network              0            0
802.11 probe request flood                                    0            0
802.11 authentication flood                                   0            0
802.11 null data flood                                        0            0
802.11 mgmt type 6 flood                                      0            0
802.11 mgmt type 7 flood                                      0            0
802.11 mgmt type d flood                                      0            0
802.11 mgmt type e flood                                      0            0
802.11 mgmt type f flood                                      0            0
802.11 association flood                                      0            0
802.11 reassociation flood                                    0            0
802.11 disassociation flood                                   0            0
Weak wep initialization vectors                               0            0
Spoofed access point mac-address attacks                      0            0
Spoofed client mac-address attacks                            0            0
Ssid masquerade attacks                                       1           12
Spoofed deauthentication attacks                              0            0
Spoofed disassociation attacks                                0            0
Null probe responses                                        626        11380
Broadcast deauthentications                                   0            0
FakeAP ssid attacks                                           0            0
FakeAP bssid attacks                                          0            0
Netstumbler clients                                           0            0
Wellenreiter clients                                          0            0
Nortel active scans                                        1796         4383
Wireless bridge frames                                      196          196
Adhoc client frames                                           8            0
access ports present in attack-list                           0            0
access ports not present in ssid-list                         0            0
access ports not present in vendor-list                       0            0
Clients not present in vendor-list                            0            0
Clients added to automatic black-list                         0            0
```

Note. WSS Software generates log messages for most of these statistics. See "IDS and DoS Alerts" on page 550.

Displaying SSID or BSSID Information for a Mobility Domain

To display SSID or BSSID information for an entire Mobility Domain, use the following command on the seed switch:

show rfdetect mobility-domain [**ssid** *ssid-name* | **bssid** *mac-addr*]

The following command displays summary information for all SSIDs and BSSIDs detected in the Mobility Domain:

```
23x0# show rfdetect mobility-domain
Total number of entries: 194
Flags: i = infrastructure, a = ad-hoc, u = unresolved
       c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
BSSID             Vendor       Type  Flags  SSID
----------------- ------------ ----- ------ --------------------------------
00:07:50:d5:cc:91        Cisco intfr i----w r27-cisco1200-2
00:07:50:d5:dc:78        Cisco intfr i----w r116-cisco1200-2
00:09:b7:7b:8a:54        Cisco intfr i-----
00:0a:5e:4b:4a:c0         3Com intfr i----- public
00:0a:5e:4b:4a:c2         3Com intfr i----w nortelwlan
00:0a:5e:4b:4a:c4         3Com intfr ic---- nrtl-ccmp
00:0a:5e:4b:4a:c6         3Com intfr i----w nrtl-tkip
00:0a:5e:4b:4a:c8         3Com intfr i----w nrtl-voip
00:0a:5e:4b:4a:ca         3Com intfr i----- nrtl-webaaa
...
```

The lines in this display are compiled from data from multiple listeners (AP radios). If an item has the value *unresolved*, not all listeners agree on the value for that item. Generally, an unresolved state occurs only when an AP or a Mobility Domain is still coming up, and lasts only briefly.

The following command displays detailed information for rogues using SSID *nrtl-webaaa*.

```
23x0# show rfdetect mobility-domain ssid nrtl-webaaa
BSSID: 00:0a:5e:4b:4a:ca Vendor: 3Com SSID:nrtl-webaaa
Type: intfr Adhoc: no Crypto-types: clear

WSS-IPaddress:10.8.121.102Port/Radio/Ch:3/1/11Mac:00:0b:0e:00:0a:6a
  Device-type: interfering Adhoc: no Crypto-types: clear
  RSSI: -85 SSID: nrtl-webaaa

BSSID: 00:0b:0e:00:7a:8a Vendor: Nortel SSID: nrtl-webaaa
Type: intfr Adhoc: no Crypto-types: clear

WSS-IPaddress:10.8.121.102Port/Radio/Ch:3/1/1Mac:00:0b:0e:00:0a:6a
  Device-type: interfering Adhoc: no Crypto-types: clear
  RSSI: -75 SSID: nrtl-webaaa

WSS-IPaddress:10.3.8.103Port/Radio/Ch:dap1/1/1Mac:00:0b:0e:76:56:82
  Device-type: interfering Adhoc: no Crypto-types: clear
  RSSI: -76 SSID: nrtl-webaaa
```

Two types of information are shown. The lines that are not indented show the BSSID, vendor, and information about the SSID. The indented lines that follow this information indicate the listeners (AP radios) that detected the SSID. Each set of indented lines is for a separate AP listener.

In this example, two BSSIDs are mapped to the SSID. Separate sets of information are shown for each of the BSSIDs, and information about the listeners for each BSSID are shown.

The following command displays detailed information for a BSSID.

```
23x0# show rfdetect mobility-domain bssid 00:0b:0e:00:04:d1
BSSID: 00:0b:0e:00:04:d1 Vendor: Cisco SSID: notmycorp
Type: rogue Adhoc: no Crypto-types: clear

WSS-IPaddress:10.8.121.102Port/Radio/Ch:3/2/56Mac:00:0b:0e:00:0a:6b
Device-type: rogue Adhoc: no Crypto-types: clear
RSSI: -72 SSID: notmycorp

WSS-IPaddress:10.3.8.103Port/Radio/Ch:dap1/1/157Mac:00:0b:0e:76:56:82
   Device-type: rogue Adhoc: no Crypto-types: clear
   RSSI: -72 SSID: notmycorp
```

Displaying RF Detect Data

To display information about the APs detected by an individual WSS switch, use the following command:

show rfdetect data

You can enter this command on any switch in the Mobility Domain.

```
23x0# show rfdetect data
Total number of entries: 197
Flags: i = infrastructure, a = ad-hoc
       c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
BSSID             Vendor  Type  Port/Radio/Ch Flags  RSSI Age SSID
----------------- ------- ----- ------------- ------ ---- --- -----------------
00:07:50:d5:cc:91   Cisco intfr       3/1/6   i----w  -61   6 r27-cisco1200-2
00:07:50:d5:dc:78   Cisco intfr       3/1/6   i----w  -82   6 r116-cisco1200-2
00:09:b7:7b:8a:54   Cisco intfr       3/1/2   i-----  -57   6
00:0a:5e:4b:4a:c0    3Com intfr       3/1/11  i-----  -57   6 public
00:0a:5e:4b:4a:c2    3Com intfr       3/1/11  i-t1--  -86   6 nortelwlan
00:0a:5e:4b:4a:c4    3Com intfr       3/1/11  ic----  -85   6 nrtl-ccmp
00:0a:5e:4b:4a:c6    3Com intfr       3/1/11  i-t---  -85   6 nrtl-tkip
00:0a:5e:4b:4a:c8    3Com intfr       3/1/11  i----w  -83   6 nrtl-voip
00:0a:5e:4b:4a:ca    3Com intfr       3/1/11  i-----  -85   6 nrtl-webaaa
...
```

Displaying the APs Detected by an AP Radio

To displays the APs detected by an AP radio, use any of the following commands:

show rfdetect visible *mac-addr*

show rfdetect visible ap *AP-num* **[radio {1 | 2}]**

show rfdetect visible dap *dap-num* **[radio {1 | 2}]**

To following command displays information about the rogues detected by radio 1 on AP port 3:

```
23x0# show rfdetect visible ap 3 radio 1
Total number of entries: 104
Flags: i = infrastructure, a = ad-hoc
       c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
Transmit MAC      Vendor  Type  Ch  RSSI Flags  SSID
----------------- ------- ----- --- ---- ------ --------------------------------
00:07:50:d5:cc:91   Cisco intfr   6  -60 i----w r27-cisco1200-2
00:07:50:d5:dc:78   Cisco intfr   6  -82 i----w r116-cisco1200-2
00:09:b7:7b:8a:54   Cisco intfr   2  -54 i-----
00:0a:5e:4b:4a:c0    3Com intfr  11  -57 i----- public
00:0a:5e:4b:4a:c2    3Com intfr  11  -86 i-t1-- nortelwlan
00:0a:5e:4b:4a:c4    3Com intfr  11  -85 ic---- nrtl-ccmp
00:0a:5e:4b:4a:c6    3Com intfr  11  -85 i-t--- nrtl-tkip
00:0a:5e:4b:4a:c8    3Com intfr  11  -83 i----w nrtl-voip
00:0a:5e:4b:4a:ca    3Com intfr  11  -85 i----- nrtl-webaaa
...
```

Displaying Countermeasures Information

To displays the current status of countermeasures against rogues in the Mobility Domain, use the following command:

show rfdetect countermeasures

This command is valid only on the Mobility Domain's seed switch.

```
23x0# show rfdetect countermeasures
Total number of entries: 190
Rogue MAC         Type  Countermeasures    WSS-IPaddr       Port/Radio
                        Radio Mac                              /Channel
----------------- ----- ------------------ --------------- -------------
00:0b:0e:00:71:c0 intfr  00:0b:0e:44:55:66 10.1.1.23       dap 4/1/6
00:0b:0e:03:00:80 rogue  00:0b:0e:11:22:33 10.1.1.23       dap 2/1/11
```

Appendix A: Troubleshooting a WS Switch

Fixing Common WSS Setup Problems 572
Recovering the System Password 574
Configuring and Managing the System Log 575
Running Traces 582
Using Show Commands 586
Remotely Monitoring Traffic 588
Capturing System Information for Technical Support 595

Some common problems that occur during WSS installation and basic configuration are simple to solve. However, to "recover" the system password, you must delete the existing WSS configuration.

System logs provide a history of WSS Software events. Traces display real-time messages from all WSS Software areas. Some **show** commands are particularly useful in troubleshooting. The **show tech-support** command combines a number of **show** commands into one, and provides an extensive snapshot of your WSS switch configuration settings for the Nortel Enterprise Technical Support (NETS).

Fixing Common WSS Setup Problems

Table 36 contains remedies for some common problems that can occur during basic installation and setup of an WSS switch.

Table 36: WSS Setup Problems and Remedies

Symptom	Diagnosis	Remedy
WLAN Management Software or a web browser (if you are using Web View) warns that the WSS switch's certificate date is invalid.	The switch's time and date are currently incorrect, or were incorrect when you generated the self-signed certificate or certificate request.	1. Use **set timezone** to set the time zone in which you are operating the switch. (See "Setting the Time Zone" on page 137.) 2. Use **set timedate** to configure the current time and date in that time zone. (See "Statically Configuring the System Time and Date" on page 139.) 3. Reconfigure the administrative certificate(s). (See Chapter , "Managing Keys and Certificates," on page 379.) 4. If you have already configured a certificate on the switch for authentication by network users, you must recreate this certificate, too.
WSS switch does not accept configuration information for an AP access point or a radio.	The country code might not be set or might be set for another country.	1. Type the **show system** command to display the country code configured on the switch. 2. If the value in the System Countrycode field is *NONE* or is for a country other than the one in which you are operating the switch, use the **set system countrycode** command to configure the correct country code. (See "Specifying the Country of Operation" on page 248.)

Table 36: WSS Setup Problems and Remedies (continued)

Symptom	Diagnosis	Remedy
Client cannot access the network.	This symptom has more than one possible cause:	
	• The client might be failing authentication or might not be authorized for a VLAN.	1. Type the **show aaa** command to ensure that the authentication rules on the WSS switch allow the client to authenticate. (See "Displaying the AAA Configuration" on page 464.) 2. Check the authorization rules in the switch's local database (**show aaa**) or on the RADIUS servers to ensure the client is authorized to join a VLAN that is configured on at least one of the WSS switches in the Mobility Domain. (See "Assigning Authorization Attributes" on page 446.) 3. Type the show **sessions command** to ensure the user is connected to the switch. 4. If user does not appear in the **sessions** list, there begin a 802.1x trace (more info on using the trace command see page 588) debug using the **set trace dot1x level 4 mac <mac address>**, and have the user reconnect, to show the trace results issue the **show log trace** command. Remember to stop all tracing when possible as it can potentially slow down the switch process. To stop the all traces type the **clear trace all** command
	• If the client and switch configurations are correct, a VLAN might be disconnected. A client connected to a disconnected VLAN is unable to access the network.	1. Type the **show vlan config** command to check the status of each VLAN. 2. If a VLAN is disconnected (VLAN state is Down), check the network cables for the VLAN's ports. At least one of the ports in a VLAN must have a physical link to the network for the VLAN to be connected.
Configuration information disappears after a software reload.	The configuration changes were not saved.	1. Retype the commands for the missing configuration information. 2. Type the **save config** command to save the changes.
Mgmt LED is quickly blinking amber. CLI stops at boot prompt (boot>).	The WSS was unable to load the system image file.	Type the **boot** command at the boot prompt.

Recovering the System Password

You can recover the system enable password if you have lost or forgotten it.

Caution! Recovering the system password will delete your configuration files.

You set the WSS switch password using the **set enablepass** command. If you forget the password, use one of the following procedures.

WSS-2350

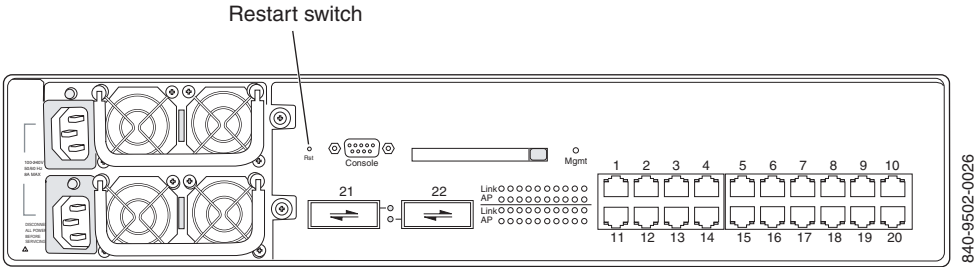
1. After the switch has fully booted, insert a pin into the factory reset switch to erase the switch's configuration.
2. Use a web browser to access IP address 192.168.100.1. This address accesses the Web Quick Start.
3. Use the Web Quick Start to set the administrator usernames and passwords and other parameters. Make sure you reconfigure the switch's IP connection.
4. See "First-Time Configuration using the Console" on page 56.

WSS-2370, WSS-2380, or WSS-2360

1. Reboot the switch, and interrupt the WSS switch boot process.

   Insert a pin into the restart switch or power the WSS switch off and on again to cause the WSS switch to reboot. Figure 22 shows the location of the restart switch on an WSS-2370 switch. The restart switch on an WSS-2360 or WSS-2380 switch is also located next to its serial console port.

Figure 22. WSS Restart Switch Location



2. When you see descending numbers on the console, press any key.
3. Type the following command at the boot> prompt:

   `boot>` **boot OPT+=default**

If you do not type the command before the reset cycle is complete, the WSS switch returns to the state it was in before you restarted it.

Once you have entered the command, the WSS switch returns to its initial unconfigured state. For information on how to configure the WSS switch, see "First-Time Configuration using the Console" on page 56.

For model WSS-2360, you also can reconfigure basic parameters using the Web Quick Start. Use a web browser to access IP address 192.168.100.1.



Caution! Use an enable password that you will remember. If you lose the password, the only way to restore it causes the system to return to its default settings and wipes out the configuration.

Configuring and Managing the System Log

System logs provide information about system events that you can use to monitor and troubleshoot WSS Software. Event messages for the WSS switch and its attached AP access points can be stored or sent to the following destinations:

- Stored in a local buffer on the WSS
- Displayed on the WSS console port
- Displayed in an active Telnet session
- Sent to one or more syslog servers, as specified in RFC 3164

The system log is a file in which the newest record replaces the oldest. These entries are preserved in nonvolatile memory through system reboots.

Log Message Components

Each log message contains the following components:

Field	Description
Facility	Portion of WSS Software that is affected
Date	Time and date the message is generated
Severity	Severity level of the message. (See Table 38: "Event Severity Levels" on page 576.)
Tag	Identifier for the message
Message	Description of the error condition

Logging Destinations and Levels

A logging destination is the location to which logged event messages are sent for storage or display. By default, only session logging is disabled. You can enable or disable logging to each destination and filter the messages by the severity of the logged event or condition. (For details, see Table 38.)

System events and conditions at different severity levels can be logged to multiple destinations. By default, events at the error level and higher are posted to the console and to the log buffer. Debug output is logged to the trace buffer by default. Table 37 summarizes the destinations and defaults for system log messages.

Table 37: System Log Destinations and Defaults

Destination	Definition	Default Operation and Severity Level
buffer	Sends log information to the nonvolatile system buffer.	Buffer is enabled and shows error-level events.
console	Sends log information to the console.	Console is enabled and shows error-level events.
current	Sends log information to the current Telnet or console session.	Settings for the type of session that the user is currently having with the WSS
server *ip-address*	Sends log information to the syslog server at the specified IP address.	Server is set during configuration and displays error-level events.
sessions	Sets defaults for Telnet sessions.	Logging is disabled and shows information-level events when enabled.
trace	Sends log information to the volatile trace buffer.	Trace is enabled and shows debug output.

Specifying a severity level sends log messages for events or conditions at that level or higher to the logging destination. Table 38 lists the severity levels and their descriptions. (For defaults, see Table 37.)

Table 38: Event Severity Levels

Severity	Description
emergency	The WSS switch is unusable.
alert	Action must be taken immediately.
critical	You must resolve the critical conditions. If the conditions are not resolved, the WSS can reboot or shut down.
error	The WSS is missing data or is unable to form a connection.
warning	A possible problem exists.
notice	Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.

Table 38: Event Severity Levels (continued)

info	Informational messages only. No problem exists.
debug	Output from debugging. **Note:** The debug level produces a lot of messages, many of which can appear to be somewhat cryptic. Debug messages are used primarily by Nortel for troubleshooting and are not intended for administrator use.

Using Log Commands

To enable, disable, or modify system logging to the WSS switch's log buffer, console, current Telnet session, or trace buffer, use the following command:

set log {**buffer** | **console** | **current** | **sessions** | **trace**} [**severity** *severity-level*] [**enable** | **disable**]

To enable, disable, or modify system logging to a syslog server, use the following command:

set log server *ip-addr* [**severity** *severity-level* [**local-facility** *facility-name*]] [**enable** | **disable**]

To view log entries in the system or trace buffer, use the following command:

show log buffer | **trace**

To clear log messages from the system or trace buffer, use the following command:

clear log buffer | **trace**

To stop sending messages to a syslog server, use the following command:

clear log server *ip-addr*

Logging to the Log Buffer

The system log consists of rolling entries stored as a last-in first-out queue maintained by the WSS. Logging to the buffer is enabled by default for events at the error level and higher.

To modify settings to another severity level, use the following command:

set log buffer severity *severity-level*

For example, to set logging to the buffer for events at the warning level and higher, type the following command:

```
23x0# set log buffer severity warning
success: change accepted.
```

To view log entries in the system log buffer, use the following command:

show log buffer [{+|-} *number-of-messages*] [**facility** *facility-name*] [**matching** *string*] [**severity** *severity-level*]

You can display the most recent messages or the oldest messages:

- Type a positive number (for example, +100) to display that number of log entries starting from the oldest in the log.
- Type a negative number (for example, -100) to display that number of log entries starting from the newest in the log.

You can search for strings by using the keyword **matching** and typing any string, such as a username or IP address.

You can display event information at a particular severity level. (See Table 38 on page 576 for information on severity levels.)

For example, the following command displays all messages at the error severity level or higher:

```
23x0# show log buffer severity error
```

```
SYSJun0217:41:35.176214ERROR nos_vms_port?add:Failedtosetdefaultvlan
v1 an:4096 for port 3 rc 1
```

To filter the event log by WSS Software area, use the **facility** *facility-name* keyword. For a list of facilities for which you can view event messages, type the following command:

```
23x0# show log buffer facility ?
<facility name>        Select one of: KERNEL, AAA, SYSLOGD, ACL, APM,
ARP,ASO,BOOT,CLI,CLUSTER,COPP,CRYPTO,DOT1X,ENCAP,ETHERNET,GATEWAY,
HTTPD, IGMP, IP, MISC, NOSE, NP, RAND, RESOLV, RIB, ROAM, ROGUE, SM, SNMPD,
SPAN,STORE,SYS,TAGMGR,TBRIDGE,TCPSSL,TELNET,TFTP,TLS,TUNNEL,VLAN,
X509, XML, AP, RAPDA, WEBVIEW, EAP, PORTCONFIG, FP.
```

To clear the buffer, type the following command:

```
23x0# clear log buffer
```

To disable logging to the system buffer, type the following command:

```
23x0# set log buffer disable
```

Logging to the Console

By default, console logging is enabled and messages at the error level and higher are sent to the console.

To modify console logging, use the following command:

set log console severity *severity-level*

(See Table 38 on page 576 for information on severity levels.)

For example, to set logging to the console for events at the critical severity level and higher, type the following command:

```
23x0# set log console severity critical
success: command accepted.
```

To disable console logging, type the following command:

```
23x0# set log console disable
success: change accepted.
```

The console is always available, but it has the following limitations:

- Console logging is slow.
- Messages logged to the console are dropped if the console output buffer overflows. WSS Software displays a message indicating the number of messages dropped.
- If you type anything to the console, the typing disables log output to the console until you press the Enter key.

Logging Messages to a Syslog Server

To send event messages to a syslog server, use the following command:

set log server *ip-addr* **severity** *severity-level* [**local-facility** *facility-name*] **enable**

Use the IP address of the syslog server to which you want messages sent. (See Table 38 on page 576 for information about severity levels.)

Use the optional **local-facility** keyword to override the default WSS Software facility numbers and replace them with one local facility number. Use the numbers 0 through 7 to map WSS Software event messages to one of the standard local log facilities *local0* through *local7* specified by RFC 3164.

If you do not specify a local facility, WSS Software sends the messages with their default WSS Software facilities. For example, AAA messages are sent with facility 4 and boot messages are sent with facility 20 by default.

For example, the following command sends all error-level event messages generated by an WSS to a server at IP address 192.168.153.09 and identifies them as facility 5 messages:

```
23x0# set log server 192.168.153.09 severity error local-facility 5
success: change accepted.
```

To stop sending log messages to a syslog server, use the following command:

clear log server *ip-addr*

To disable logging to the server, use the following command:

set log server *ip-addr* **disable**

Setting Telnet Session Defaults

Session logging is disabled by default, and the event level is set to information (info) or higher. To enable event logging to Telnet sessions and change the default event severity level, use the following command:

set log sessions severity *severity-level* **enable**

(For information on severity levels, see Table 38 on page 576.)

To disable session logging, use the following command:

set log sessions disable

Changing the Current Telnet Session Defaults

By default, log information is not sent to your current Telnet session, and the log level is set to information (info) or higher. To modify the severity of events logged to your current Telnet session, use the following command from within the session:

set log current severity *severity-level*

(For information about severity levels, see Table 38 on page 576.)

To enable current session logging, type the following command:

```
23x0# set log current enable
success: change accepted
```

To disable current session logging, type the following command:

```
23x0# set log current disable
success: change accepted
```

Logging to the Trace Buffer

Trace logging is enabled by default and stores debug-level output in the WSS trace buffer. To modify trace logging to an event level higher than debug, use the following command:

set log trace severity *severity-level*

To disable trace logging, use the following command:

```
set log trace disable
success: change accepted.
```

(To display the trace log, see "Stopping a Trace" on page 583. For information about the trace function, see "Running Traces" on page 582.)

Saving Trace Messages in a File

To save the accumulated trace data for enabled traces to a file in the WSS switch's nonvolatile storage, use the following command:

save trace *filename*

To save trace data into the file *trace1* in the subdirectory *traces*, type the following command:

```
23x0# save trace traces/trace1
```

Displaying the Log Configuration

To display your current log configuration, type the following command:

```
23x0# show log config
Logging console:                enabled
Logging console severity:       INFO
Logging sessions:               enabled
Logging sessions severity:      INFO
Logging buffer:                 enabled
Logging buffer severity:        ERROR
Logging buffer size:            400 messages
Logging trace:                  enabled
Logging trace severity:         DEBUG
Logging buffer size:            1048576 bytes

Logging server:               192.168.253.11  severity CRITICAL

Current session:                disabled
Current session severity:         INFO
```

Running Traces

Trace commands enable you to perform diagnostic routines. You can set a trace command with a keyword, such as **authentication** or **sm**, to trace activity for a particular feature, such as authentication or the session manager.



Warning! Using the **set trace** command can have adverse effects on system performance. Nortel recommends that you use the lowest levels possible for initial trace commands, and slowly increase the levels to get the data you need.

Using the Trace Command

Tracing is used only for debugging WSS Software. The command **set trace** *area* enables you to view messages about the status of a specific portion of the WSS Software.

There are many trace parameters that you can run. (See "List of Trace Areas" on page 585.) However, this chapter describes only authentication, authorization, the session manager (**sm**), and 802.1X users (**dot1x**), four areas that you might find most helpful.

To focus on the object of the trace, you can add one or more of these parameters to the **set trace** command:

set trace [*area*] [**mac-addr** *mac-addr*] [**port** *port-num*] [**user** *username*] [**level** *level*]

Tracing Authentication Activity

Tracing authentication activity can help you diagnose authentication problems. You can trace all authentication activity, or only the activity for a specific user, MAC address, or port.

For example, to trace all authentication activity at level 4, type the following command:

```
23x0# set trace authentication level 4
success: change accepted.
```

Tracing Session Manager Activity

You can trace all session manager commands, or only those for a specific user, MAC address, or port. For example, to trace all session manager (**sm**) activity at level 3, type the following command:

```
23x0# set trace sm level 3
success: change accepted.
```

Tracing Authorization Activity

Tracing authorization activity can help diagnose authorization problems. For example, to trace the authorization of MAC address 00:00:30:b8:72:b0, type the following command:

```
23x0# set trace authorization mac-addr 00:00:30:b8:72:b0
success: change accepted.
```

Tracing 802.1X Sessions

Tracing 802.1X sessions can help diagnose problems with wireless clients. For example, to trace 802.1X activity for user tamara@example.com at level 4, type the following command:

```
23x0# set trace dot1x user tamara@example.com level 4
success: change accepted.
```

Displaying a Trace

Use the **show trace** command to show the trace areas that are enabled. For example, to display all currently running trace commands, type the following command:

```
23x0# show trace
milliseconds spent printing traces: 31.945
Trace Area           Level Mac               User              Port Filter
-------------------- ----- ----------------- ----------------- ---- --------
authentication           3                   admin                       0
authorization            5                                               0
sm                       5                                    11         0
dot1x                    2                                               0
```

Stopping a Trace

The **clear trace** commands deletes running trace commands. To clear all traces or a particular trace area, type the following command:

clear trace {**all** | *trace area*}

(For a list of all areas that can be traced, see "List of Trace Areas" on page 585.)

For example, to stop a trace of session manager activity, type the following command:

```
23x0# clear trace sm
success: change accepted.
```

About Trace Results

The trace commands use the underlying logging mechanism to deliver trace messages. Trace messages are generated with the debug severity level. By default, the only log target that receives debug-level messages is the volatile trace buffer. (To see the contents of the trace buffer, see "Displaying Trace Results" on page 584.)

The volatile trace buffer receives messages for all log severities when any trace area is active. However, if no trace area is active, no messages are sent to the trace buffer regardless of their severity. If you do not enable trace commands, the trace buffer is effectively disabled.

Because traces use the logging facility, any other logging target can be used to capture trace messages if its severity is set to debug. However, since tracing can be voluminous, Nortel discourages this in practice. To enable trace output to the console, enter the command **set log console severity debug**.

If you attempt to send trace output to a Telnet session, be aware that tracing is disabled for areas processing packets that might be associated with the Telnet session.

Displaying Trace Results

To view the output of currently running trace commands, use the following command:

show log trace [{+|-|/}*number-of-messages*] [**facility** *facility-name*] [**matching** *string*] [**severity** *severity-level*]

For example, the following command displays a trace log of error-level events:

```
23x0# show log trace severity error
KERNELJan1523:08:10ERRORduplicateIPaddress10.7.122.102sentfromlink
address 00:05:5d:45:ae:cd
```

To display a specific number of trace log messages, you must enter a plus sign (+), minus sign (-), or slash (/) before the number. These characters filter the messages displayed as follows:

+*number-of-messages*	Displays the specified number of log entries, starting with the oldest in the log.
-*number-of-messages*	Displays the specified number of entries, starting with the newest in the log.
/*number-of-messages*	Displays the specified number of the most recent entries in the log, starting with the least recent.

To filter trace output by WSS Software area, use the **facility** *facility-name* keyword. For a list of valid facilities for which you can view event messages, type the following command:

```
23x0# show log trace facility ?
<facility name>        Select one of: KERNEL, AAA, SYSLOGD, ACL, APM,
ARP,ASO,BOOT,CLI,CLUSTER,COPP,CRYPTO,DOT1X,ENCAP,ETHERNET,GATEWAY,
HTTPD, IGMP, IP, MISC, NOSE, NP, RAND, RESOLV, RIB, ROAM, ROGUE, SM, SNMPD,
SPAN,STORE,SYS,TAGMGR,TBRIDGE,TCPSSL,TELNET,TFTP,TLS,TUNNEL,VLAN,
X509, XML, AP, RAPDA, WEBVIEW, EAP, PORTCONFIG, FP.
```

Copying Trace Results to a Server

To copy the contents of the trace buffer to a file on a TFTP server, use the following command:

copy *trace-buffer-name* **tftp://**[*destination-ip-addr* | *destination-hostname*]/*destination-filename*

To find the name of the trace buffer file, use the **dir** command.

For example, the following command copies the log messages in trace buffer 0000000001 to a TFTP server at IP address 192.168.253.11, in a file called *log-file*:

```
23x0# copy 0000000001 tftp://192.168.253.11/log-file
```

Clearing the Trace Log

To clear all messages from the trace log buffer, type the following command:

```
23x0# clear log trace
```

List of Trace Areas

To see all WSS Software areas you can trace, type the following command:

```
23x0# set trace ?
```

Using Show Commands

To troubleshoot the WSS switch, you can use **show** commands to display information about different areas of the WSS Software. The following commands can provide helpful information if you are experiencing WSS Software performance issues.

Viewing VLAN Interfaces

To view interface information for VLANs, type the following command:

WSS-2370# show interface

```
* = From DHCP
VLAN Name            Address         Mask            Enabled State RIB
---- --------------- --------------- --------------- ------- ----- --------
   1 default         0.0.0.0         0.0.0.0         NO      Down  ipv4
 130 vlan-eng        192.168.12.7    255.255.255.0   YES     Up    ipv4
 190 vlan-wep        192.168.19.7    255.255.255.0   YES     Up    ipv4
```

(For more information about VLAN interfaces, see "Configuring and Managing VLANs" on page 88.)

Viewing AAA Session Statistics

To view AAA session statistics, type the following command:

23x0# show aaa

```
Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=5 key=(null) author-pass=(null)

Radius Servers
Server                   Addr           Ports   T/o Tries Dead State
-------------------------------------------------------------------------
SQA2BServer           11.1.1.11       1812 1813  5    3    5    UP
SideShow              192.168.0.21    1812 1813  5    3    0    UP
   Server groups
    sg1: SideShow
    SQA: SQA2BServer
set authentication dot1x *@xAPl.com pass-through sg1
set authentication dot1x *@xAPl.com pass-through SQA
set authentication dot1x EXAMPLE\* peap-mschapv2 sg1

user sqa
   password = 08325d4f (encrypted)
   session-timeout = 3600

mac-user 00:00:a6:47:ad:03
   session-timeout = 3600
```

```
      vlan-name = vlan-wep
   mac-user 00:00:65:16:0d:69
      session-timeout = 3600
      vlan-name = vlan-eng
```

(For more information about AAA, see Chapter , "Configuring AAA for Administrative and Local Access," on page 51 and Chapter , "Configuring AAA for Network Users," on page 401.)

Viewing FDB Information

The **show fdb** command displays the hosts learned by the WSS switch and the ports to which they are connected. To display forwarding database (FDB) information, type the following command:

23x0# **show fdb**

```
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG  Dest MAC/Route Des [CoS]  Destination Ports or VCs/[Protocol Type]
---- ---- ------------------ ----- ------------------------------------------
 130    3 00:05:5d:7e:94:83                 1                          [ALL]
 130  130 00:02:2d:85:6b:4d                 t:192.168.14.6             [ALL]
 130  130 00:0b:0e:12:34:56                 t:192.168.15.5             [ALL]
 130  130 00:0b:0e:02:76:f6                 t:192.168.14.6             [ALL]
 130    2 00:02:2d:86:bd:38                 3                          [ALL]
 130    3 00:05:5d:84:d3:d3                 1                          [ALL]
4097      00:0b:0e:00:04:30     #           CPU                        [ALL]
4096      00:0b:0e:00:04:30     #           CPU                        [ALL]
130      00:0b:0e:00:04:30      #           CPU                        [ALL]
Total Matching FDB Entries Displayed = 32
dynamic = 27, static=0, permanent=0, system=5
```

(For more information about forwarding databases, see "Managing the Layer 2 Forwarding Database" on page 96.)

Viewing ARP Information

The **show arp** command displays the ARP aging timer and ARP entries in the system. To display ARP information, type the following command:

23x0# **show arp**

```
ARP aging time: 1200 seconds
Host                          HW Address         VLAN  Type    State
----------------------------- ----------------- ----- ------- --------
10.8.1.1                      00:30:b6:3e:5c:a8     1 DYNAMIC RESOLVED
10.8.107.1                    00:0b:0e:00:04:0c     1 LOCAL   RESOLVED
```

(For more information about ARP, see "Managing the ARP Table" on page 147.)

Remotely Monitoring Traffic

Remote traffic monitoring enables you to snoop wireless traffic, by using a Distributed AP as a sniffing device. The AP copies the sniffed 802.11 packets and sends the copies to an observer, which is typically a protocol analyzer such as Ethereal or Tethereal.

How Remote Traffic Monitoring Works

To monitor wireless traffic, an AP radio compares traffic sent or received on the radio to snoop filters applied to the radio by the network administrator. When an 802.11 packet matches all conditions in a filter, the AP encapsulates the packet in a Tazmen Sniffer Protocol (TZSP) packet and sends the packet to the observer host IP addresses specified by the filter. TZSP uses UDP port 37008 for its transport. (TZSP was created by Chris Waters of Network Chemistry.)

You can map up to eight snoop filters to a radio. A filter does not become active until you enable it. Filters and their mappings are persistent and remain in the configuration following a restart. However, filter state is not persistent. If the switch or the AP is restarted, the filter is disabled. To continue using the filter, you must enable it again.

Using Snoop Filters on Radios That Use Active Scan

When active scan is enabled in a radio profile, the radios that use the profile actively scan other channels in addition to the data channel that is currently in use. Active scan operates on enabled radios and disabled radios. In fact, using a disabled radio as a dedicated scanner provides better rogue detection because the radio can spend more time scanning on each channel.

When a radio is scanning other channels, snoop filters that are active on the radio also snoop traffic on the other channels. To prevent monitoring of data from other channels, use the **channel** option when you configure the filter, to specify the channel on which you want to scan.

All Snooped Traffic Is Sent in the Clear

Traffic that matches a snoop filter is copied after it is decrypted. The decrypted (clear) version is sent to the observer.

Best Practices for Remote Traffic Monitoring

- Do not specify an observer that is associated with the AP where the snoop filter is running. This configuration causes an endless cycle of snoop traffic.
- If the snoop filter is running on a Distributed AP, and the AP used a DHCP server in its local subnet to configure its IP information, and the AP did not receive a default gateway address as a result, the observer must also be in the same subnet. Without a default gateway, the AP cannot find the observer.
- The AP that is running a snoop filter forwards snooped packets directly to the observer. This is a one-way communication, from the AP to the observer. If the observer is not present, the AP still sends the snoop packets, which use bandwidth. If the observer is present but is not listening to TZSP traffic, the observer continuously sends ICMP error indications back to the AP. These ICMP messages can affect network and AP performance.

To inform you of this condition, WSS Software generates a log message such as the following the first time an ICMP error message is received following the start of a snoop filter:

```
AP Mar 25 13:15:21.681369 ERROR DAP 3 ap_network: Observer
10.10.101.2 is not accepting TZSP packets
```

To prevent ICMP error messages from the observer, Nortel recommends using the Netcat application on the observer to listen to UDP packets on the TZSP port.

Configuring a Snoop Filter

To configure a snoop filter, use the following command:

set snoop *filter-name* [*condition-list*] [**observer** *ip-addr*] [**snmp-length** *num*]

The *filter-name* can be up to 32 alphanumeric characters.

The *condition-list* specifies the match criteria for packets. Conditions in the list are ANDed. Therefore, to be copied and sent to an observer, a packet must match all criteria in the *condition-list*. You can specify up to eight of the following conditions in a filter, in any order or combination:

frame-type {**eq** | **neq**} {**beacon** | **control** | **data** | **management** | **probe**}

channel {**eq** | **neq**} *channel*

bssid {**eq** | **neq**} *bssid*

src-mac {**eq** | **neq**} *mac-addr*

dest-mac {**eq** | **neq**} *mac-addr*

host-mac {**eq** | **neq**} *mac-addr*

mac-pair *mac-addr1 mac-addr2*

To match on packets to or from a specific MAC address, use the **dest-mac** or **src-mac** option. To match on both send and receive traffic for a host address, use the **host-mac** option. To match on a traffic flow (source and destination MAC addresses), use the **mac-pair** option. This option matches for either direction of a flow, and either MAC address can be the source or destination address.

If you omit a condition, all packets match that condition. For example, if you omit **frame-type**, all frame types match the filter.

For most conditions, you can use **eq** (equal) to match only on traffic that matches the condition value. Use **neq** (not equal) to match only on traffic that is not equal to the condition value.

The **observer** *ip-addr* option specifies the IP address of the station where the protocol analyzer is located. If you do not specify an observer, the AP radio still counts the packets that match the filter. (See "Displaying Remote Traffic Monitoring Statistics" on page 594.)

The **snap-length** *num* option specifies the maximum number of bytes to capture. If you do not specify a length, the entire packet is copied and sent to the observer. Nortel recommends specifying an snap length of 100 bytes or less.

The following command configures a snoop filter named *snoop1* that matches on all traffic, and copies the traffic to the device that has IP address 10.10.30.2:

```
23x0# set snoop snoop1 observer 10.10.30.2 snap-length 100
```

The following command configures a snoop filter named *snoop2* that matches on all data traffic between the device with MAC address aa:bb:cc:dd:ee:ff and the device with MAC address 11:22:33:44:55:66, and copies the traffic to the device that has IP address 10.10.30.3:

```
23x0# set snoop snoop2 frame-type eq data mac-pair aa:bb:cc:dd:ee:ff 11:22:33:44:55:66
    observer 10.10.30.3 snap-length 100
```

Displaying Configured Snoop Filters

To display the snoop filters configured on the WSS switch, use the following command:

show snoop info [*filter-name*]

The following command shows the snoop filters configured in the examples above:

```
23x0# show snoop info
snoop1:
        observer 10.10.30.2 snap-length 100
        all packets
snoop2:
        observer 10.10.30.3 snap-length 100
        frame-type eq data
        mac-pair (aa:bb:cc:dd:ee:ff, 11:22:33:44:55:66)
```

Editing a Snoop Filter

To edit a snoop filter, you can use the **show configuration area snoop** command to display the filter's configuration command, then use cut-and-paste to reconstruct the command.

Deleting a Snoop Filter

To delete a snoop filter, use the following command:

clear snoop *filter-name*

Mapping a Snoop Filter to a Radio

You can map a snoop filter to a radio on a Distributed AP. To map a snoop filter to a radio, use the following command:

set snoop map *filter-name* **dap** *dap-num* **radio** {**1** | **2**}

You can map the same filter to more than one radio. You can map up to eight filters to the same radio. If more than one filter has the same observer, the AP sends only one copy of a packet that matches a filter to the observer. After the first match, the AP sends the packet and stops comparing the packet against other filters for the same observer.

If the filter does not have an observer, the AP still maintains a counter of the number of packets that match the filter. (See "Displaying Remote Traffic Monitoring Statistics" on page 594.)

The following command maps snoop filter *snoop1* to radio 2 on Distributed AP 3:

```
23x0# set snoop map snoop1 dap 3 radio 2
success: change accepted.
```

Displaying the Snoop Filters Mapped to a Radio

To display the snoop filters that are mapped to a radio, use the following command:

show snoop map *filter-name*

The following command shows the mapping for snoop filter *snoop1*:

```
23x0# show snoop map snoop1
filter 'snoop1' mapping
        Dap: 3          Radio: 2
```

Displaying the Snoop Filter Mappings for All Radios

To display all snoop filter mappings, use the following command:

```
23x0# show snoop
Dap: 3          Radio: 2
        snoop1
        snoop2
Dap: 2          Radio: 2
        snoop2
```

Removing Snoop Filter Mappings

To remove a snoop filter from a specific radio, use the following command:

clear snoop map *filter-name* **dap** *dap-num* **radio {1 | 2}**

The following command removes snoop filter *snoop2* from radio 2 on Distributed AP 3:

```
23x0# clear snoop map snoop2 dap 3 radio 2
success: change accepted.
```

To remove all snoop filter mappings from all radios, use the following command:

clear snoop map all

Enabling or Disabling a Snoop Filter

A snoop filter does not take effect until you enable it. To enable or disable a snoop filter, use the following command:

set snoop {*filter-name* | all}
mode {**enable** [**stop-after** *num-pkts*] | **disable**}

The **stop-after** option disables the filter after the specified number of packets match the filter. Without the **stop-after** option, the filter operates until you disable it or until the AP is restarted.

Note. The filter mode is not retained if you change the filter configuration or disable and reenable the radio, or when the AP or the WSS switch is restarted. You must reenable the filter to place it back into effect.

The following command enables snoop filter *snoop1*, and configures the filter to stop after 5000 packets match the filter:

```
23x0# set snoop snoop1 mode enable stop-after 5000
success: filter 'snoop1' enabled
```

Displaying Remote Traffic Monitoring Statistics

The AP collects statistics for packets that match the enabled snoop filters mapped to its radios. The AP retains statistics for a snoop filter until the filter is changed or disabled. The AP then clears the statistics.

To display statistics for packets matching a snoop filter, use the following command:

show snoop stats [*filter-name* [*dap-num* [**radio** {**1** | **2**}]]]

The following command shows statistics for snoop filter *snoop1*:

```
23x0# show snoop stats snoop1
Filter          Dap Radio   Rx Match     Tx Match     Dropped        Stop-After
================================================================================
snoop1            3     1            96           4           0       stopped
```

Preparing an Observer and Capturing Traffic

To observe monitored traffic, install the following applications on the observer:

- Ethereal or Tethereal Version 0.10.8 or later
- Netcat (any version), if not already installed

Ethereal and Tethereal decode 802.11 packets embedded in TZSP without any configuration.

Use Netcat to listen to UDP packets on the TZSP port. This avoids a constant flow of ICMP destination unreachable messages from the observer back to the radio. You can obtain Netcat through the following link:

http://www.securityfocus.com/tools/139/scoreit

If the observer is a PC, you can use a Tcl script instead of Netcat if preferred.

1. Install the required software on the observer.
2. Configure and map snoop filters in WSS Software.
3. Start Netcat, using a command such as the following:

   nc -l -u -p 37008 ip-addr > /dev/null &

   Where *ip-addr* is the IP address of the Distributed AP to which the snoop filter is mapped. (To display the Distributed AP's IP address, use the **show dap status** command.)
4. Start the capture application:
   - For Ethereal capture, use **ethereal filter port 37008**.
   - For Tethereal capture, use **tethereal -V port 37008**.
5. Disable the option to decrypt 802.11 payloads. Because the AP always decrypts the data before sending it to the observer, the observer does not need to perform any decryption. In fact, if you leave decryption enabled on the observer, the payload data becomes unreadable.

   To disable the decryption option in Ethereal:

   a. In the decode window, right-click on the *IEEE 802.11* line.
   b. Select **Protocol Preferences** to display the 802.11 Protocol Preferences dialog.
   c. Click next to **Ignore the WEP bit** to deselect the option. This option is applicable for any type of data encryption used by AP radios.

6 Enable the snoop filter on the AP, using the following command:

set snoop {*filter-name* | `all`} **mode** {**enable** [**stop-after** *num-pkts*] | **disable**}

7 Stop the Ethereal capture and view the monitored packets.

The source IP address of a monitored packet identifies the Distributed AP that copied the packet's payload and sent it to the observer.

Capturing System Information for Technical Support

For problems you cannot solve yourself, use the **show tech-support** command to generate a report of your WSS switch's configuration and status, which you can show to NETS.

Displaying Technical Support Information

The **show tech-support** command combines a group of show commands to provide an in-depth snapshot of the status of the WSS. The output displays details about the system image and configuration used after the last reboot, the version, ports, AAA settings, and other configuration values, and the last 100 log messages.

Run this command before calling the Nortel Enterprise Technical Support (NETS). See "How to get Help" on page 29 and "Sending Information to NETS" on page 597 for more information.

Sending Information to NETS

NETS might request that you create a copy of the output from the **show tech-support** command. If NETS requests you to do so, follow these steps:

1. Type the command with a filename. For example:

   23x0# **show tech-support file fortechsupport**
   `success: results saved to fortechsupport.gz`

2. Copy the file to the TFTP server. Type the following command using the TFTP address and filename given to you by NETS:

   23x0# **copy fortechsupport.gz tftp://***tftpserver/filename.gz*

3. Email *filename.gz* to your NETS representative.

Appendix B: Supported RADIUS Attributes

Supported Standard and Extended Attributes 599
Nortel Vendor-Specific Attributes 603

Nortel WLAN 2300 System Software (WSS Software) supports the standard and extended RADIUS authentication and accounting attributes listed in Table 39. Also supported are Nortel vendor-specific attributes (VSAs), listed in Table 40 on page 604.

An attribute is sent to RADIUS accounting only if the table listing it shows *Yes* or *Optional* in the column marked *Sent in Accounting-Request* for the attribute *and* the attribute is applied to the client's session configuration. Attribute values have the following characteristics unless otherwise stated:

- Strings can contain a maximum of 253 characters.
- Integers are 4 bytes.
- IP addresses are 4 bytes.

The RADIUS attributes WSS Software supports are based on these IETF RFCs and drafts:

- RFC 2865, *Remote Authentication Dial-in User Service (RADIUS)*
- RFC 2866, *RADIUS Accounting*
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*
- RFC 2869, *RADIUS Extensions*
- *draft-congdon-radius-8021x-29.txt* (*IEEE 802.1X RADIUS Usage Guidelines*)

Supported Standard and Extended Attributes

The RADIUS attributes shown in Table 39 are sent by WSS switches to RADIUS servers during authentication and accounting.

Table 39: 801.1X Attributes

Attribute	Type	Rcv in Access Resp?	Sent in Access Reqst?	Sent in Acct Reqst?	Description and Values
User-Name	1	No	Yes	Yes	String. Name of the user to be authenticated. Used only in Request packets.
User-Password	2	No	Yes	No	Password of the user to be authenticated, unless a CHAP-Password is used.
CHAP-Password	3	No	Yes	No	Password of the user to be authenticated, unless a User-Password is used.
NAS-IP-Address	4	No	Yes	Yes	IP address sent by the WSS switch.
Service-Type	5	No	Yes	Yes	Access type, which can be one of the following: • 2—Framed; for network user access • 6—Administrative; for administrative access to the WSS switch, with authorization to access the enabled (configuration) mode. The user must enter the **enable** command and the correct enable password to access the enabled mode. • 7—NAS-Prompt; for administrative access to the nonenabled mode only. In this mode, the user can still enter the **enable** command and the correct enable password to access the enabled mode. For administrative sessions, the WSS switch always sends 6 (Administrative). The RADIUS server can reply with one of the values listed above. If the service-type is not set on the RADIUS server, administrative users receive NAS-Prompt access, and network users receive Framed access.
Filter-Id	11	Yes	No	Optional	Name of an access control list (ACL) to filter outbound or inbound traffic. Use the form *ACL name***.in** and *ACL name***.out**. (For details, see Chapter , "Configuring and Managing Security ACLs," on page 351.)

Table 39: 801.1X Attributes (continued)

Attribute	Type	Rcv in Access Resp?	Sent in Access Reqst?	Sent in Acct Reqst?	Description and Values
Reply-Message	18	Yes	No	No	String. Text that can be displayed to the user. Multiple Reply-Messages can be included. If any are displayed, they must appear in the order in which they appear in the packet.
State	24	Yes	Yes	No	Can be sent by a RADIUS server in an Access-Challenge message to the WSS switch. If the WSS receives an Access-Challenge with this attribute, it returns the same State value in an Access-Request response to the RADIUS server, when a response is required. (For details, see RFC 2865.)
Class	25	Yes	No	Yes	If received, this information must be sent on, without interpretation, in all subsequent packets sent to the RADIUS server for that client session.
Vendor-Specific	26	Yes	No	Yes	String. Allows WSS Software to support Nortel VSAs. (See Table 40 on page 604.)
Session-Timeout	27	Yes	No	Optional	Maximum number of seconds of service allowed the user before reauthentication of the session.
Called-Station-Id	30	No	Yes	Yes	For IEEE 802.1X authenticators, stores the AP access point MAC address in uppercase ASCII format, with octet values separated by hyphens (for example, 00-10-A4-23-19-C0).
Calling-Station-Id	31	No	Yes	Yes	For IEEE 802.1X authenticators, stores the supplicant MAC address in uppercase ASCII format, with octet values separated by hyphens (for example, 00-10-A4-23-19-C0).
NAS-Identifier	32	No	Yes	No	Name of the RADIUS client originating an Access-Request. The value in the current release is **Nortel** and cannot be changed.
Acct-Status-Type	40	No	No	Yes	Valid values: • Acct-Start • Acct-Interim-Update • Acct-Stop
Acct-Delay-Time	41	No	No	Yes	Time in seconds for which the client has been trying to send the record.

Table 39: 801.1X Attributes (continued)

Attribute	Type	Rcv in Access Resp?	Sent in Access Reqst?	Sent in Acct Reqst?	Description and Values
Acct-Input-Octets	42	No	No	Yes	Number of octets received from the port over the course of this service being provided. Can be present only in Accounting-Request records in which Acct-Status-Type is set to Acct-Stop or Acct-Interim-Update.
Acct-Output-Octets	43	No	No	Yes	Number of octets sent on the port in the course of this service being provided. Can be present only in Accounting-Request records in which Acct-Status-Type is set to Acct-Stop or Acct-Interim-Update.
Acct-Session-Id	44	No	No	Yes	Unique accounting ID to facilitate matching start and stop records in a log file. The start and stop records for a given session must have the same Acct-Session-Id.
Acct-Authentic	45	No	No	Yes	Valid values: • RADIUS • Local
Acct-Session-Time	46	No	No	Yes	Number of seconds for which the user has received service. Can be present only in Accounting-Request records in which Acct-Status-Type is set to Acct-Stop or Acct-Interim-Update.
Acct-Input-Packets	47	No	No	Yes	Number of packets received in the course of this service being provided. Can be present only in Accounting-Request records in which Acct-Status-Type is set to Acct-Stop or Acct-Interim-Update.
Acct-Output-Packets	48	No	No	Yes	Number of packets sent in the course of this service being provided. Can be present only in Accounting-Request records in which Acct-Status-Type is set to Acct-Stop or Acct-Interim-Update.
Acct-Multi-Session-Id	50	No	No	Yes	Unique accounting ID that facilitates linking together multiple related sessions in a log file. Each linked session has a unique Acct-Session-Id but the same Acct-Multi-Session-Id.

Table 39: 801.1X Attributes (continued)

Attribute	Type	Rcv in Access Resp?	Sent in Access Reqst?	Sent in Acct Reqst?	Description and Values
Acct-Input-Gigawords	52	No	No	Yes	Number of times the Acct-Input-Octets counter has wrapped around 2^{32} over the course of this service being provided. Can be present only in Accounting-Request records in which Acct-Status-Type is set to Acct-Stop or Acct-Interim-Update. (For details, see RFC 2869.)
Acct-Output-Gigawords	53	No	No	Yes	Number of times the Acct-Output-Octets counter has wrapped around 2^{32} over the course of this service being provided. Can be present only in Accounting-Request records in which Acct-Status-Type is set to Acct-Stop or Acct-Interim-Update. (For details, see RFC 2869.)
Event-Timestamp	55	No	No	Yes	Time that the user session started, stopped, or was updated, in seconds since January 1, 1970.
Tunnel-Private-Group-ID	81	Yes	No	No	Same as VLAN-Name.
NAS-Port-Id	87	No	Yes	Yes	WSS physical port that authenticates the user, in the form *AP port number/radio*.

Nortel Vendor-Specific Attributes

The vendor-specific attributes (VSAs) created by Nortel are embedded according to the procedure recommended in RFC 2865, with Vendor-ID set to 562. Table 40 on page 604 describes the Nortel VSAs, listed in order by vendor type number.

(For attribute details, see Table 32: "Authentication Attributes for Local Users" on page 446.)

Table 40: Nortel VSAs

Attribute	Type, Vendor ID, Vendor Type	Rcv in Access Resp?	Sent in Access Reqst?	Sent in Acct Reqst?	Description
VLAN-Name	26, 562, 1	Yes	No	Yes	Name of the VLAN to which the client belongs.
Mobility-Profile	26, 562, 2	Yes	No	No	Name of the Mobility Profile used by the authorized client.
Encryption-Type	26, 562, 3	Yes	No	No	Type of encryption used to authenticate the client.
Time-Of-Day	26, 562, 4	Yes	No	No	Day(s) and time(s) during which a user can log into the network.
SSID	26, 562, 5	Yes	No	Yes	Name of the SSID you want the user to use. The SSID must be configured in a service profile, and the service profile must be used by a radio profile assigned to Nortel radios in the Mobility Domain.
End-Date	26, 562, 6	Yes	No	No	Date and time after which the user is no longer allowed to be on the network. Use the following format: YY/MM/DD-HH:MM
Start-Date	26, 562, 7	Yes	No	No	Date and time at which the user becomes eligible to access the network. Use the following format: YY/MM/DD-HH:MM
URL	26, 562, 8	Yes	No	No	URL to which the user is redirected after successful Web-based AAA. Use the following format: http://www.example.com

Appendix C: Mobility Domain Traffic Ports

When deploying a Mobility Domain, you might attach the WSS switches to subnets that have firewalls or access controls between them. Within a Mobility Domain, WSS switches exchange information and other types of traffic, depending on your configuration of AAA and various management services.

Table 41 lists the traffic ports typically used by a Mobility Domain and its associated AAA and management functions.

Table 41: Traffic Ports for AAA Servers and Management Servers

Protocol	Port	Function
IP/UDP (17)	1812	RADIUS authentication (default setting)
IP/UDP (17)	1813	RADIUS accounting (default setting)
IP/TCP (6)	443	SSL management through Web View
IP/TCP (6)	8889	SSL management through WMS
IP/TCP (6)	23	Telnet management
IP/UDP (17)	161	SNMP get and set operations
IP/UDP (17)	162	SNMP traps
IP/ICMP (1)	N/A	Several types (for example, ping)
IP/UDP (17)	123	NTP
IP/UDP (17)	53	DNS

The traffic typically sent between WSS switches within a Mobility Domain uses IP/UDP protocol 17 traffic on port 8817 for both source and destination. Roaming traffic uses IP protocol 4.

Appendix D: DHCP Server

How the WSS Software DHCP Server Works 608
Configuring the DHCP Server 608
Displaying DHCP Server Information 609

WSS Software has a DHCP server that the switch uses to allocate IP addresses to the following:

- Directly connected APs
- Host connected to a new (unconfigured) WSSR-2350 or WSS-2360, to configure the switch using the Web Quick Start

DHCP service for these items is enabled by default.

Optionally, you can configure the DHCP server to also provide IP addresses to Distributed APs and to clients.

Configuration is supported on an individual VLAN basis. When you configure the DHCP server on a VLAN, the server can serve addresses only from the subnet that contains the host address assigned to the VLAN. By default, the VLAN can serve any unused address in the subnet except the VLAN's host address and the network and broadcast addresses. You can specify the address range.

You can configure the DHCP server on more than one VLAN. You can configure a DHCP client and DHCP server on the same VLAN, but only the client or the server can be enabled. The DHCP client and DHCP server cannot both be enabled on the same VLAN at the same time.

The WSS Software DHCP server is implemented according to "RFC 2131: Dynamic Host Configuration Protocol" and "RFC 2132: DHCP Options and BOOTP Vendor Extensions", with the following exceptions:

- If the switch is powered down or restarted, WSS Software does not retain address allocations or lease times.
- The WSS Software DHCP server will not operate properly when another DHCP server is present on the same subnet.
- The WSS Software DHCP server is configurable on an individual VLAN basis only, and operates only on the subnets for which you configure it.



Note. Use of the WSS Software DHCP server to allocate client addresses is intended for temporary, demonstration deployments and not for production networks. Nortel recommends that you do not use the WSS Software DHCP server to allocate client addresses in a production network.

How the WSS Software DHCP Server Works

When WSS Software receives a DHCP Discover packet, the DHCP server allocates an address from the configured range according to RFC 2131 and ARPs the address to ensure that it is not already in use. If the address is in use, the server allocates the next address in the range, and ARPs again. The process continues until WSS Software finds an address that is not in use. WSS Software then offers the address to the Distributed AP or client that sent the DHCP Discover. If there are no unused addresses left in the range, WSS Software ignores the DHCP Discover and generates a log message.

If the client does not respond to the DHCP Offer from the WSS Software DHCP server within 2 minutes, the offer becomes invalid and WSS Software returns the address to the pool.

The siaddr value in the DHCP exchanges is the IP address of the VLAN. The yiaddr value is an unused address within the range the server is allowed to use.

In addition to an IP address, the Offer message from the WSS Software DHCP server also contains the following options:

- Option 54—Server Identifier, which has the same value as siaddr.
- Option 51—Address Lease, which is 12 hours and cannot be configured.
- Option 1—Subnet Mask of the VLAN's IP interface.
- Option 15—Domain Name, which is the default domain name configured on the switch. If the default domain name is not configured, this option is blank.
- Option 3—Router. If the IP route table contains a default route with an address in the subnet configured on the VLAN, then the server specifies this address. Otherwise, the server does not specify a router address.
- Option 6—Domain Name Server, which is a list of the DNS server IP addresses configured on the switch. If no DNS servers are configured on the switch, this option is blank.

Configuring the DHCP Server

You can configure the DHCP server on an individual VLAN basis. To configure the server, use the following command:

set interface *vlan-id* **ip dhcp-server** [**enable** | **disable**] [**start** *ip-addr1* **stop** *ip-addr2*]

The *vlan-id* can be the VLAN name or number.

The **start** *ip-addr1* and **stop** *ip-addr2* options specify the beginning and ending addresses of the address range (also called the address *pool*). By default, all addresses except the host address of the VLAN, the network broadcast address, and the subnet broadcast address are included in the range. If you specify the range, the start address must be lower than the stop address, and all addresses must be in the same subnet. The IP interface of the VLAN must be within the same subnet but is not required to be within the range.

The following command enables the DHCP server on VLAN *red-vlan* to serve addresses from the 192.168.1.5 to 192.168.1.25 range:

```
23x0# set interface red-vlan ip dhcp-server enable start 192.168.1.5 stop 192.168.1.25
success: change accepted.
```

To remove all IP information from a VLAN, including the DHCP client and user-configured DHCP server, use the following command:

clear interface *vlan-id* **ip**



Note. This command clears all IP configuration information from the interface.

Displaying DHCP Server Information

To display information about the WSS Software DHCP server, use the following command:

show dhcp-server [interface *vlan-id***] [verbose]**

If you enter the command without the interface or verbose option, the command displays a table of all the IP addresses leased by the server. You can use the **interface** option to display addresses leased by a specific VLAN.

If you use the **verbose** option, configuration and status information is displayed instead.

The following command displays the addresses leased by the DHCP server:

```
23x0# show dhcp-server
VLAN Name            Address         MAC               Lease Remaining (sec)
---- --------------- --------------- ----------------- --------------------
   1 default         10.10.20.2      00:01:02:03:04:05                 12345
   1 default         10.10.20.3      00:01:03:04:06:07                  2103
   2 red-vlan        192.168.1.5     00:01:03:04:06:08                   102
   2 red-vlan        192.168.1.7     00:01:03:04:06:09                 16789
```

The following command displays configuration and status information for each VLAN on which the DHCP server is configured:

```
23x0# show dhcp-server
Interface:         0 (Direct AP)
 Status:            UP
 Address Range:     10.0.0.1-10.0.0.253

 Interface:             default(1)
 Status:                UP
 Address Range:         10.10.20.2-10.10.20.254
 DHCP Clients:
   Hardware Address:      00:01:02:03:04:05
   State:                 BOUND
   Lease Allocation:      43200 seconds
   Lease Remaining:       12345 seconds
   IP Address:            10.10.20.2
   Subnet Mask:           255.255.255.0
   Default Gateway:       10.10.20.1
   DNS Servers:           10.10.20.4 10.10.20.5
   DNS Domain Name:       mycorp.com
```

In addition to information for addresses leased from the VLANs where you configured the server, information for the Direct AP interface is also displayed. The Direct AP interface is an internal VLAN interface for directly connected APs.

Glossary

3DES A three-round application of the Data Encryption Standard (DES) that uses a 168-bit encryption key. See also *DES*.

802.1D The IEEE LAN specification for the operation of media access control (MAC) bridges.

802.1p An IEEE LAN standard method for classifying packets in bridged virtual LANs (VLANs). As part of 802.1Q protocol, 802.1p defines a field in the VLAN tag of a frame header that provides class-of-service (CoS) definitions at Layer 2. See also *802.1Q*.

802.1Q The IEEE LAN standard that defines a protocol for filtering and forwarding services at Layer 2. Ethernet frames are directed by means of a tag inserted into the frame header. A virtual LAN (VLAN) identifier (VID) field in the tag identifies the VLAN with which the frame is associated.

802.1X The primary IEEE standard for port-based network access control. The 802.1X standard, which is based on the Extensible Authentication Protocol (EAP), provides an authentication framework that supports a variety of methods for authenticating and authorizing network access for wired or wireless users. See also *EAP*; *EAP-TLS*; *PEAP*; *TLS*; *TTLS*.

802.2 An IEEE LAN specification that defines the logical link control (LLC) sublayer, the upper portion of the Data Link layer. LLC encapsulation can be used by any lower-layer LAN technology. Compare *802.3*; *Ethernet II*.

802.3 An IEEE LAN specification for a Carrier Sense Multiple Access with Collision Detection (CSMA-CD) network, a type of network related to Ethernet. In general, 802.3 specifies the physical media and the working characteristics of LANs. An 802.3 frame uses source and destination media access control (MAC) addresses to identify its originator and receiver (or receivers). Compare *802.2*; *Ethernet II*.

802.3z An extension to the IEEE 802.3 LAN specification, describing gigabit Ethernet (1000 Mbps) transmission. The extension includes specifications for the media access control (MAC), physical layer, repeater, and management characteristics of gigabit Ethernet.

802.11 An IEEE LAN specification that defines the mobile (wireless) network access link layer. The specification includes the 802.11 media access control (MAC) sublayer of the Data Link layer, and two sublayers of the Physical (PHY) layer—a frequency-hopping spread-spectrum (FHSS) physical layer and a direct-sequence spread-spectrum (DSSS) link layer. Later additions to 802.11 include additional physical layers. See also *802.11a*; *802.11b*; *802.11g*; *802.11i*.

802.11a A supplement to the IEEE 802.11 wireless LAN (WLAN) specification, describing transmission through the Physical layer (PHY) based on orthogonal frequency division multiplexing (OFDM), at a frequency of 5 GHz and data rates of up to 54 Mbps.

802.11b A supplement to the IEEE 802.11 wireless LAN (WLAN) specification, describing transmission through the Physical layer (PHY) based on direct-sequence spread-spectrum (DSSS), at a frequency of 2.4 GHz and data rates of up to 11 Mbps.

802.11b/g radio A radio that can receive and transmit signals at IEEE 802.11b and 802.11g data rates. Nortel 802.11b/g radios allow associations from 802.11b clients as well as 802.11g clients by default, for networks that have a mixture of both client types. However, association by any 802.11b clients restricts the maximum data transmit rate for all clients. To allow the radios to operate at the higher 802.11g data rates, you can set 802.11b/g radios to reject association attempts by 802.11b clients.

802.11g A supplement to the IEEE 802.11 wireless LAN (WLAN) specification, describing transmission through the Physical layer (PHY) based on orthogonal frequency division multiplexing (OFDM), at a frequency of 2.4 GHz and data rates of up to 54 Mbps.

802.11i A draft supplement to the IEEE 802.11 wireless LAN (WLAN) specification, for enhanced security through the use of stronger encryption protocols such as the Temporal Key Integrity Protocol (TKIP) and AES Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). These protocols provide replay protection, cryptographically keyed integrity checks, and key derivation based on the IEEE 802.1X port authentication standard. See also *AES*; *CCMP*; *TKIP*; *WPA*.

AAA Authentication, authorization, and accounting. A framework for configuring services that provide a secure network connection and a record of user activity, by identifying who the user is, what the user can access, and what services and resources the user is consuming. In a Nortel WLAN 2300 System, the WLAN—Security Switch (WSS) switch can use a RADIUS server or its own local database for AAA services.

access control entry See ***ACE***.

access control list See *security ACL*.

Access Point (AP) A small hardware unit that functions as a wireless access point (AP) in a Nortel WLAN 2300 System. Using one or more radio transmitters, an AP transmits and receives information as radio frequency (RF) signals to and from a wireless user (client). The AP transmits and receives information over a 10/100BASE-T Ethernet connection to and from a WLAN—Security Switch (WSS) switch. The switch also supplies electrical power to the access point by means of Power over Ethernet (PoE). An optional dual-homed connection to a second WSS provides redundancy. An AP communicates with an WSS by means of the Nortel access point Access (TAPA) protocol.

ACE A rule in a security access control list (ACL) that grants or denies a set of network access rights based on one or more criteria. ACEs use criteria such as a protocol and a source or destination IP address to determine whether to permit or deny packets that match the criteria. ACEs are processed in the order in which they appear in the security ACL. See also *security ACL*.

ACL See *security ACL*.

ad hoc network One of two IEEE 802.11 network frameworks. In an ad hoc network, a set of wireless stations communicate directly with one another without using an access point (AP) or any connection to a wired network. With an ad hoc network, also known as a *peer-to-peer network* or *independent basic service set (IBSS)*, you can set up a wireless network in which a wireless infrastructure does not exist or is not required for services (in a classroom, for example), or through which access to the wired network is prevented (for consultants at a client site, for example). Compare *infrastructure network*.

Advanced Encryption Standard See *AES*.

AES Advanced Encryption Standard. One of the Federal Information Processing Standards (FIPS). The AES, documented in FIPS Publication 197, specifies a symmetric encryption algorithm for use by organizations to protect sensitive information. See *802.11i*; *CCMP*.

AP See *Access Point (AP)*.

association The process defined in IEEE 802.11 by which an authenticated mobile (wireless) station establishes a relationship with a wireless access point (AP) to gain full network access. The access point assigns the mobile station an association identifier (AID), which the wireless LAN (WLAN) uses to track the mobile station as it roams. After associating with a Access Point (AP) access point in a Nortel WLAN 2300 System, a mobile station can send and receive traffic through any AP access point within the same Mobility Domain™ group.

attribute In authentication, authorization, and accounting (AAA), a property used to identify (authenticate) a user or to configure (authorize) or record (account for) a user's administrative or network session. A user's AAA attributes are stored in a user profile in the local database on a WLAN—Security Switch (WSS) switch, or on a RADIUS server. Attribute names are case-sensitive. See also *RADIUS*; *VSA*.

authenticated identity In a Nortel WLAN 2300 System, the correspondence established between a user and his or her authentication attributes. User authentication attributes are linked to the *user*, rather than to a physical port or device, regardless of the user's location or type of network connection. Because the authenticated identity follows the user, he or she requires no reauthentication when roaming.

authentication, authorization, and accounting See *AAA*.

authentication mobility The ability of a user (client) authenticated through Extensible Authentication Protocol (EAP)—plus an appropriate subprotocol and back-end authentication, authorization, and accounting (AAA) service—to roam to different access points (APs) without reauthentication.

authentication server An entity that provides an authentication service to an authenticator. From the credentials provided by a client (or *supplicant*), the authentication service determines whether the supplicant is authorized to access the services of the authenticator. In a Nortel WLAN 2300 System, one or more RADIUS servers can act as authentication servers.

authenticator A device that authenticates a client. In a Nortel WLAN 2300 System, the authenticator is a WLAN—Security Switch (WSS) switch.

baseline association rate A value set in Nortel WMS to help plan Access Point (AP) access point coverage in a network. The baseline association rate is the average data transmission rate at which you want typical mobile clients in the coverage area to associate with the access point(s).

basic service set See *BSS*.

basic service set identifier See *BSSID*.

bias The priority of one Wireless Security Switch (WSS) switch over other WSS switches for booting, configuring, and providing data transfer for a Access Point (AP) access port. Bias can be set to either low or high on each WSS switch and is high by default. Bias applies only to WSS switches that are indirectly attached to the AP through an intermediate Layer 2 or Layer 3 network. An AP always attempts to boot on AP port 1 first, and if the AP is directly attached to an WSS switch on AP port 1, the AP uses the directly attached WSS switch to boot from regardless of the bias settings. See also *dual-homed connection*.

BSS Basic service set. A set of wireless stations that communicate with one another through an access point (AP).

BSSID Basic service set identifier. The 48-bit media access control (MAC) address of the radio in the access point (AP) that serves the stations in a basic service set (BSS).

CA See *certificate authority (CA)*.

CBC-MAC See *CCMP*.

CCI Co-channel interference. Obstruction that occurs when one signal on a particular frequency intrudes into a cell that is using that same frequency for transmission. In multicell networks, systems are designed to minimize CCI through appropriate transmission power and channel selection.

CCMP Counter-Mode with Cipher Block Chaining Message Authentication Code Protocol. A wireless encryption protocol based on the Advanced Encryption Standard (AES) and defined in the IEEE 802.11i specification. CCMP uses a symmetric key block cipher mode that provides privacy by means of counter mode and data origin authenticity by means of cipher block chaining message authentication code (CBC-MAC). See also *802.11i*; *AES*; *TKIP*; *WPA*. Compare *WEP*.

cell The geographical area covered by a wireless transmitter.

certificate authority (CA) Network software that issues and manages security credentials and public keys for authentication and message encryption. As part of a public-key infrastructure (PKI), which enables secure exchanges of information over a network, a certificate authority checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the registration authority verifies the requestor's information, the certificate authority can issue a certificate. Based on the PKI implementation, the certificate content can include the certificate's expiration date, the owner's public key, the owner's name, and other information about the public-key owner. See also *registration authority (RA)*.

Certificate Signing Request See *CSR*.

Challenge Handshake Authentication Protocol See *CHAP*.

CHAP Challenge Handshake Authentication Protocol. An authentication protocol that defines a three-way handshake to authenticate a user (client). CHAP uses the MD5 hash algorithm to generate a response to a challenge that can be checked by the authenticator. For wireless connections, CHAP is not secure and must be protected by the cryptography in such authentication methods as the Protected Extensible Authentication Protocol (PEAP) and Tunneled Transport Layer Security (TTLS).

client The requesting program or device in a client-server relationship. In a wireless LAN (WLAN), the client (or *supplicant*) requests access to the services provided by the authenticator. See also *supplicant*.

co-channel interference See *CCI*.

collision domain A single half-duplex IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA-CD) network. A collision occurs when two or more Layer 2 devices in the network transmit at the same time. Ethernet segments separated by a Layer 2 switch are within different collision domains.

comma-separated values file See *CSV file*.

communications plenum cable See *plenum-rated cable*.

coverage area In Nortel WMS, the smallest unit of floor space within which to plan access point coverage for a wireless LAN (WLAN). The number of access ports required for a coverage area depends on the type of IEEE 802.11 transmission used, and the area's physical features and user density.

CPC Communications plenum cable. See *plenum-rated cable*.

CRC Cyclic redundancy check. A primitive message integrity check.

crypto See *cryptography*.

cryptography The science of information security. Modern cryptography is typically concerned with the processes of scrambling ordinary text (known as *plain text* or *clear text*) into encrypted text at the sender's end of a connection, and decrypting the encrypted text back into clear text at the receiver's end. Because its security is independent of the channels through which the text passes, cryptography is the only way of protecting communications over channels that are not under the user's control. The goals of cryptography are *confidentiality*, *integrity*, *nonrepudiation*, and *authentication*. The encrypted information cannot be understood by anyone for whom it is not intended, or altered in storage or transmission without the alteration being detected. The sender cannot later deny the creation or transmission of the information, and the sender and receiver can confirm each other's identity and the information's origin and destination.

CSR Certificate Signing Request. A message sent by an administrator to request a security certificate from a certificate authority (CA). A CSR is a text string formatted by Privacy-Enhanced Mail (PEM) protocol according to Public Key Cryptography Standard (PKCS) #10. The CSR contains the information needed by the certificate authority to generate the certificate.

CSV file Comma-separated values file. A text file that displays tabular data in a comma-delimited format, as a list of rows in which each column's value is separated from the next by a comma. A CSV file is useful for transferring data between database applications.

cyclic redundancy check See *CRC*.

dBm Decibels referred to 1 milliwatt (mW). A measurement of relative power related to 1 mW. For example, *20 dBm* corresponds to $10^{20\ dBm/10} = 100\ mW$.

decibels referred to 1 milliwatt (mW). See *dBm*.

Data Encryption Standard See *DES*.

delivery traffic indication map See *DTIM*.

DES Data Encryption Standard. A federally approved symmetric encryption algorithm in use for many years and replaced by the Advanced Encryption Standard (AES). See also *3DES*.

DHCP Dynamic Host Configuration Protocol. A protocol that dynamically assigns IP addresses to stations, from a centralized server. DHCP is the successor to the Bootstrap Protocol (BOOTP).

dictionary attack An attempt to gain illegal access to a computer or network by logging in repeatedly with passwords that are based on a list of terms in a dictionary.

Diffie-Hellman A key exchange algorithm that was the first public-key algorithm ever published. Diffie-Hellman can be used anonymously (without authentication). Anonymous Diffie-Hellman is used to establish the connection between the Nortel WLAN 2300 System WLAN Management Software tool suite and a WLAN—Security Switch (WSS) switch.

Diffserv Differentiated services. An architecture for providing different types or levels of service for network traffic. Diffserv aggregates flows in the network so that routers and switches need to distinguish only a relatively small number of aggregated flows, even if those flows contain thousands or millions of individual flows.

digital certificate A document containing the name of a user (client) or server, a digital signature, a public key, and other elements used in authentication and encryption. See also *X.509*.

digital signature The result of encrypting a hash of a message or document with a private key. A digital signature is used to verify the authenticity of the sender and the integrity (unaltered condition) of the message or document. See also *hash*.

Digital Signature Algorithm See *DSA*.

direct-sequence spread-spectrum See *DSSS*.

domain (1) On the Internet, a set of network addresses that are organized in levels. (2) In Microsoft Windows NT and Windows 2000, a set of network resources (applications, printers, and so forth) for a group of users (clients). Clients log into the domain to access the resources, which can be located on a number of different servers in the network.

domain policy A collection of configuration settings that you can define once in WLAN Management Software and apply to many WLAN—Security Switch (WSS) switches. Each Mobility Domain group in the network has a default domain policy that applies to every WSS switch in the Mobility Domain. See also *Policy Manager*.

DSA Digital Signature Algorithm. The public-key algorithm used to sign X.509 certificates.

DSSS Direct-sequence spread-spectrum. One of two types of spread-spectrum radio technology used in wireless LAN (WLAN) transmissions. To increase a data signal's resistance to interference, the signal at the sending station is combined with a higher-rate bit sequence that spreads the user data in frequency by a factor equal to the spreading ratio. Compare *FHSS*.

DTIM Delivery traffic indication map. A special type of traffic indication map (TIM) element in a beacon frame that occurs only when a station in a basic service set (BSS) is in power-save mode. A DTIM indicates that any buffered broadcast or multicast frames are immediately transmitted by an access point (AP).

DXF format A tagged data representation, in ASCII format, of the information contained in an AutoCAD drawing file.

dual-homed connection A redundant, resilient connection between an Access Point (AP) and one or more Wireless Security Switch (WSS) switches. The connection can consist of two direct physical links from both AP ports to one or two WSS switches, one or more distributed links through an intermediate Layer 2 or Layer 3 network, or a combination of one direct physical link and one or more distributed links. The AP uses one link for booting, configuration, and data transfer and uses the other link(s) as backups in case the active link fails. If the AP has two direct physical links to one or more WSSs , the Power over Ethernet (PoE) load is shared across both links. If the active data link fails, the other link provides uninterrupted power to the AP access port.

After changing its active link, the access point reboots and loads new configuration information to ensure proper configuration and security. Mobility Domain services are temporarily disrupted by the link change. Dual-homed connections are not required but are recommended. See also *bias*.

EAP Extensible Authentication Protocol. A general point-to-point protocol that supports multiple authentication mechanisms. Defined in RFC 2284, EAP has been adopted by IEEE 802.1X in an encapsulated form for carrying authentication messages in a standard message exchange between a user (client) and an authenticator. The encapsulated EAP, also known as *EAP over LAN (EAPoL)* and *EAP over Wireless (EAPoW),* enables the authenticator's server to authenticate the client with an authentication protocol agreed upon by both parties. See also *EAP type*.

EAPoL EAP over LAN. An encapsulated form of the Extensible Authentication Protocol (EAP), defined in the IEEE 802.1X standard, that allows EAP messages to be carried directly by a LAN media access control (MAC) service between a wireless client (or *supplicant*) and an authenticator. EAPoL is also known as *EAP over Wireless (EAPoW)*. See also *EAP*.

EAP over LAN See *EAPoL*.

EAP over Wireless See *EAPoL*.

EAPoW See *EAPoL*.

EAP-TLS Extensible Authentication Protocol with Transport Layer Security. An EAP subprotocol for 802.1X authentication. EAP-TLS supports mutual authentication and uses digital certificates to fulfill the mutual challenge. When a user (client) requests access, the authentication server responds with a server certificate. The client replies with its own certificate and also validates the server certificate. From the certificate values, the EAP-TLS algorithm can derive session encryption keys. After validating the client certification, the authentication server sends the session encryption keys for a particular session to the client. Compare *PEAP*.

EAP type A specific Extensible Authentication Protocol (EAP) authentication mechanism. Both the wireless client (or *supplicant*) and the authenticator must support the same EAP type for successful authentication to occur. EAP types supported in a Nortel WLAN 2300 System wireless LAN (WLAN) include EAP-MD5, EAP-TLS, PEAP-TLS, PEAP-MS-CHAP, and Tunneled Transport Layer Security (TTLS). See also *MD5*; *MS-CHAP-V2*; *PEAP*; *TLS*; *TTLS*.

EAP with Transport Layer Security See *EAP-TLS*.

enabled access Permission to use all WLAN 2300 System Software (WSS Software) command-line interface (CLI) commands required for configuration and troubleshooting. Enabled access requires a separate enable password. Compare *restricted access*.

encryption Any procedure used in cryptography to translate data into a form that can be read by only its intended receiver. An encrypted signal must be decrypted to be read. See also *cryptography*.

ESS Extended service set. A logical connection of multiple basic service sets (BSSs) connected to the same network. Roaming within an ESS is guaranteed by the Nortel WLAN 2300 System.

Ethernet II The original Ethernet specification produced by Digital, Intel, and Xerox (DIX) that served as the basis of the IEEE 802.3 standard.

ETSI European Telecommunications Standards Institute. A nonprofit organization that establishes telecommunications and radio standards for Europe.

European Telecommunications Standards Institute See *ETSI*.

extended service set See *ESS*.

Extensible Authentication Protocol See *EAP*.

Extensible Markup Language See *XML*.

failover In a redundant system, an operation by which a standby (or secondary) system component automatically takes over the functions of an active (or primary) system component when the active component fails or is temporarily shut down or removed for servicing. During and after failover, the system continues its normal operations with little or no interruption in service.

FCC Federal Communications Commission. The United States' governing body for telecommunications, radio, television, cable, and satellite communications.

FDB See *forwarding database (FDB)*.

Federal Communications Commission See *FCC*.

FHSS Frequency-hopping spread-spectrum. One of two types of spread-spectrum radio technology used in wireless LAN (WLAN) transmissions. The FHSS technique modulates the data signal with a narrowband carrier signal that "hops" in a predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. Interference is reduced, because a narrowband interferer affects the spread-spectrum signal only if both are transmitting at the same frequency at the same time. The transmission frequencies are determined by a spreading (*hopping*) code. The receiver must be set to the same hopping code and must listen to the incoming signal at the proper time and frequency to receive the signal. Compare *DSSS*.

forwarding database (FDB) A database maintained on a WLAN—Security Switch (WSS) switch for the purpose of making Layer 2 forwarding and filtering decisions. Each entry consists of the media access control (MAC) address of a source or destination device, an identifier for the port on which the source or destination station is located, and an identifier for the virtual LAN (VLAN) to which the device belongs. FDB entries are either permanent (never deleted), static (not aged, but deleted when the WSS is restarted or loses power), or dynamic (learned dynamically and removed through aging or when the WSS is restarted or loses power).

frequency-hopping spread-spectrum See *FHSS*.

GBIC Gigabit interface converter. A hot-swappable input/output device that plugs into a gigabit Ethernet port, to link the port with a fiber-optic or copper network. The data transfer rate is 1 gigabit per second (Gbps) or more. Typically employed as high-speed interfaces, GBICs allow you to easily configure and upgrade communications networks.

gigabit interface converter See *GBIC*.

wildcard See *MAC address wildcard*; *user wildcard*; *VLAN wildcard*.

GMK Group master key. A cryptographic key used to derive a group transient key (GTK) for the Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

greenfield network An original deployment of a telecommunications network.

GRE tunnel A virtual link between two remote points on a network, created by means of the Generic Routing Encapsulation (GRE) tunneling protocol. GRE encapsulates packets within a transport protocol supported by the network.

GTK Group transient key. A cryptographic key used to encrypt broadcast and multicast packets for transmissions using the Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

group master key See *GMK*.

group transient key See *GTK*.

H.323 A set of International Telecommunications Union Telecommunication Standardization Sector (ITU-T) standards that define a framework for the transmission of real-time voice signals over IP packet-switched networks.

hash A one-way algorithm from whose output the input is computationally infeasible to determine. With a good hashing algorithm you can produce identical output from two identical inputs, but finding two different inputs that produce the same output is computationally infeasible. Hash functions are used widely in authentication algorithms and for key derivation procedures.

HiperLAN High-performance radio local area network. A set of wireless LAN (WLAN) communication standards used primarily in European countries and adopted by the European Telecommunications Standards Institute (ETSI).

HMAC Hashed message authentication code. A function, defined in RFC 2104, for keyed hashing for message authentication. HMAC is used with MD5 and the secure hash algorithm (SHA).

hashed message authentication code See *HMAC*.

Hewlett-Packard Open View See *HPOV*.

homologation The process of certifying a product or specification to verify that it meets regulatory standards.

HPOV Hewlett-Packard Open View. The umbrella network management system (NMS) family of products from Hewlett-Packard. The Nortel WLAN 2300 System WLAN Management Software tool suite interacts with the HPOV Network Node Manager (NNM).

HTTPS Hypertext Transfer Protocol over Secure Sockets Layer. An Internet protocol developed by Netscape to encrypt and decrypt network connections to Web servers. Built into all secure browsers, HTTPS uses the Secure Sockets Layer (SSL) protocol as a sublayer under the regular HTTP application layer, and uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP. See also *SSL*.

Hypertext Transfer Protocol over Secure Sockets Layer See *HTTPS*.

IAS Internet Authentication Service. Microsoft's RADIUS server.

IC Industry Canada. The Canadian governing body for telecommunications.

ICV Integrity check value. The output of a message integrity check.

IE See *WPA IE*.

IEEE Institute of Electrical and Electronic Engineers. An American professional society whose standards for the computer and electronics industry often become national or international standards. In particular, the IEEE 802 standards for LANs are widely followed.

IGMP Internet Group Management Protocol. An Internet protocol, defined in RFC 2236, that enables an Internet computer to report its multicast group membership to neighboring multicast routers. Multicasting allows a computer on the Internet to send content to other computers that have identified themselves as interested in receiving it.

IGMP snooping A feature that prevents the flow of multicast stream packets within a virtual LAN (VLAN) and forwards the multicast traffic through a path to only the clients that want to receive it. A Wireless Security Switch (WSS) switch uses IGMP snooping to monitor the Internet Group Management Protocol (IGMP) conversation between hosts and routers. When the WSS detects an IGMP report from a host for a given multicast group, it adds the host's port number to the list for that group. When it detects an IGMP host leaving a group, the WSS removes the port number from the group list.

Industry Canada See *IC*.

information element See *WPA IE*.

infrastructure network One of two IEEE 802.11 network frameworks. In an infrastructure network, all communications are relayed through an access point (AP). Wireless devices can communicate with each other or with a wired network. The network is defined by the distance of mobile stations from the access port, but no restriction is placed on the distance between stations. Stations must request association with the access point to obtain network services, which the access point can grant or deny based on the contents of the association request. Like most corporate wireless LANs (WLANs), which must access a wired LAN for file servers and printers, a Nortel WLAN 2300 System is an infrastructure network. Compare *ad hoc network*.

initialization vector (IV) In encryption, random data used to make a message unique.

Institute of Electrical and Electronic Engineers See *IEEE*.

integrity check value See *ICV*.

interface A place at which independent systems meet and act on or communicate with each other, or the means by which the interaction or communication is accomplished.

International Organization for Standardization See *ISO*.

Internet Authentication Service See *IAS*.

Internet Group Management Protocol See *IGMP*.

Interswitch Link See *ISL*.

ISL Interswitch Link. A proprietary Cisco protocol for interconnecting multiple switches and maintaining virtual LAN (VLAN) information as traffic travels between switches. Working in a way similar to VLAN trunking, described in the IEEE 802.1Q standard, ISL provides VLAN capabilities while maintaining full wire-speed performance on Ethernet links in full-duplex or half-duplex mode. ISL operates in a point-to-point environment and supports up to 1000 VLANs.

ISO International Organization for Standardization. An international organization of national standards bodies from many countries. ISO has defined a number of computer standards, including the Open Systems Interconnection (OSI) standardized architecture for network design.

IV See *initialization vector (IV)*.

jumbo frame In an Ethernet network, a frame whose data field exceeds 1500 bytes.

LAWN See *WLAN*.

LDAP Lightweight Directory Access Protocol. A protocol defined in RFC 1777 for management and browser applications that require simple read-write access to an X.500 directory without incurring the resource requirements of Directory Access Protocol (DAP). Protocol elements are carried directly over TCP or other transport, bypassing much of the session and presentation overhead. Many protocol data elements are encoded as ordinary strings, and all protocol elements are encoded with lightweight basic encoding rules (BER).

Lightweight Directory Access Protocol See *LDAP*.

location policy An ordered list of rules that overrides the virtual LAN (VLAN) assignment and security ACL filtering applied to users during normal authentication, authorization, and accounting (AAA)—or assigns a VLAN or security ACL to users without these assignments. Defining location policy rules creates a location policy for local access within a Wireless Security Switch (WSS) switch. Each WSS switch can have only one location policy. See also *location policy rule*.

location policy rule A rule in the location policy on a WLAN—Security Switch (WSS) switch that grants or denies a set of network access rights based on one or more criteria. Location policy rules use a username or VLAN membership to determine whether to override—or supply—authorization attributes during authentication and to redirect traffic. Location policy rules are processed in the order in which they appear in the location policy. See also *location policy*.

MAC (1) Media access control. See *MAC address*. (2) Message authentication code. A *keyed hash* used to verify message integrity. In a keyed hash, the key and the message are inputs to the hash algorithm. See also *MIC*.

MAC address Media access control address. A 6-byte hexadecimal address that a manufacturer assigns to the Ethernet controller for a port. Higher-layer protocols use the MAC address at the MAC sublayer of the Data Link layer (Layer 2) to access the physical media. The MAC function determines the use of network capacity and the stations that are allowed to use the medium for transmission.

MAC address wildcard A Nortel convention for matching media access control (MAC) addresses or sets of MAC addresses by means of known characters plus a "wildcard" asterisk (*) character that stands for from 1 byte to 5 bytes of the address. See also *user wildcard*; *VLAN wildcard*.

MAC protocol data unit See *MPDU*.

MAC service data unit See *MSDU*.

managed device In a Nortel WLAN 2300 System wireless LAN (WLAN), a Wireless Security Switch (WSS) switch or Access Point (AP) access point under the control of the WLAN Management Software tool suite.

master secret A code derived from the pre-master secret. A master secret is used to encrypt Transport Layer Security (TLS) authentication exchanges and also to derive a pairwise master key (PMK). See also *PMK*; *pre-master secret*.

maximum transmission unit See *MTU*.

MD5 Message-digest algorithm 5. A one-way hashing algorithm used in many authentication algorithms and also to derive cryptographic keys in many algorithms. MD5 takes a message of an arbitrary length and creates a 128-bit message digest.

media access control address See *MAC address*.

message authentication code See *MAC*.

message-digest algorithm 5 See *MD5*.

message integrity code See *MIC*.

MIC Message integrity code. The IEEE term for a message authentication code (MAC). See *MAC*.

Microsoft Challenge Handshake Authentication Protocol See *MS-CHAP-V2*.

minimum data transmit rate The lowest rate at which a Access Point (AP) access point can transmit data to its associated mobile clients. If the data rate to a client drops below the minimum, the AP increases power, if RF Auto-Tuning is enabled.

Mobility Domain™ A collection of Wireless Security Switch (WSS) switches working together to support a roaming user (client).

Wireless Security Switch™ (WSS™) A switch in a Nortel WLAN 2300 System. An WSS provides forwarding, queuing, tunneling, and some security services for the information it receives from its directly attached Access Point (AP) access ports. In addition, the WSS coordinates, provides power to, and manages the configuration of each attached AP, by means of the Nortel access point Access (TAPA) protocol.

Mobility Profile™ A user (client) authorization attribute that specifies the Access Point (AP) access ports or wired authentication ports the client can use in a Mobility Domain™ group.

MPDU MAC protocol data unit. In IEEE 802.11 communications, the data unit (or *frame*) that two peer media access control (MAC) service access ports (SAPs) exchange through the services of the Physical layer (PHY). An APDU consists of MAC headers and a MAC service data unit (MSDU). See also *MSDU*.

MS-CHAP-V2 Microsoft Challenge Handshake Authentication Protocol version 2. Microsoft's extension to CHAP. MS-CHAP-V2 is a mutual authentication protocol, defined in RFC 2759, that also permits a single login in a Microsoft network environment. See also *CHAP*.

MSDU MAC service data unit. In IEEE 802.11 communications, the data payload encapsulated within a MAC protocol data unit (APDU).

WSS Software See *WLAN 2300 System Software™ (WSS Software™)*.

MTU Maximum transmission unit. The size of the largest packet that can be transmitted over a particular medium. Packets exceeding the MTU value in size are fragmented or segmented, and then reassembled at the receiving end. If fragmentation is not supported or possible, a packet that exceeds the MTU value is dropped.

NAT Network address translation. The capability, defined in RFC 3022, of using one set of reusable IP addresses for internal traffic on a LAN, and a second set of globally unique IP addresses for external traffic.

network address translation See *NAT*.

network plan A design for network deployment and settings for network configuration, stored in the Nortel WLAN 2300 System WLAN Management Software tool suite.

nonvolatile storage A way of storing images and configurations so that they are maintained in a unit's memory whether power to the unit is on or off.

Odyssey An 802.1X security and access control application for wireless LANs (WLANs), developed by Funk Software, Inc.

OFDM Orthogonal frequency division multiplexing. A modulation technique that sends data across a number of narrow subcarriers within a specified frequency band. The wireless networking standards IEEE 802.11a and IEEE 802.11g are based on OFDM.

orthogonal frequency division multiplexing See *OFDM*.

pairwise master key See *PMK*.

pairwise transient key See *PTK*.

PAT Port address translation. A type of network address translation (NAT) in which each computer on a LAN is assigned the same IP address, but a different port number. See also *NAT*.

PEAP Protected Extensible Authentication Protocol. A draft extension to the Extensible Authentication Protocol with Transport Layer Security (EAP-TLS), developed by Microsoft Corporation, Cisco Systems, and RSA Data Security, Inc. TLS is used in PEAP Part 1 to authenticate the server only, and thus avoids having to distribute user certificates to every client. PEAP Part 2 performs mutual authentication between the EAP client and the server. Compare *EAP-TLS*.

PEM Privacy-Enhanced Mail. A protocol, defined in RFC 1422 through RFC 1424, for transporting digital certificates and certificate signing requests over the Internet. PEM format encodes the certificates on the basis of an X.509 hierarchy of certificate authorities (CAs). Base64 encoding is used to convert the certificates to ASCII text, and the encoded text is enclosed between BEGIN CERTIFICATE and END CERTIFICATE delimiters.

Per-VLAN Spanning Tree protocol See *PVST+*.

PIM Protocol Independent Multicast protocol. A protocol-independent multicast routing protocol that supports thousands of groups, a variety of multicast applications, and existing Layer 2 subnetwork technologies. PIM can be operated in two modes: dense and sparse. In PIM dense mode (PIM-DM), packets are flooded on all outgoing interfaces to many receivers. PIM sparse mode (PIM-SM) limits data distribution to a minimal number of widely distributed routers. PIM-SM packets are sent only if they are explicitly requested at a rendezvous point (RP).

PKCS Public-Key Cryptography Standards. A group of specifications produced by RSA Laboratories and secure systems developers, and first published in 1991. Among many other features and functions, the standards define syntax for digital certificates, certificate signing requests, and key transportation.

PKI Public-key infrastructure. Software that enables users of an insecure public network such as the Internet to exchange information securely and privately. The PKI uses public-key cryptography (also known as *asymmetric cryptography*) to authenticate the message sender and encrypt the message by means of a pair of cryptographic keys, one public and one private. A trusted certificate authority (CA) creates both keys simultaneously with the same algorithm. A registration authority (RA) must verify the certificate authority before a digital certificate is issued to a requestor.

The PKI uses the digital certificate to identify an individual or an organization. The private key is given only to the requesting party and is never shared, and the public key is made publicly available (as part of the digital certificate) in a directory that all parties can access. You use the private key to decrypt text that has been encrypted with your public key by someone else. The certificates are stored (and, when necessary, revoked) by directory services and managed by a certificate management system. See also *certificate authority (CA)*; *registration authority (RA)*.

plenum A compartment or chamber to which one or more air ducts are connected.

plenum-rated cable A type of cable approved by an independent test laboratory for installation in ducts, plenums, and other air-handling spaces.

PMK Pairwise master key. A code derived from a master secret and used as an encryption key for IEEE 802.11 encryption algorithms. A PMK is also used to derive a pairwise transient key (PTK) for IEEE 802.11i robust security. See also *master secret*; *PTK*.

PoE Power over Ethernet. A technology, defined in the developing IEEE 802.3af standard, to deliver DC power over twisted-pair Ethernet data cables rather than power cords. The electrical current, which enters the data cable at the power-supply end and comes out at the device end, is kept separate from the data signal so neither interferes with the other.

policy A formal set of statements that define the way a network's resources are allocated among its clients—individual users, departments, host computers, or applications. Resources are statically or dynamically allocated by such factors as time of day, client authorization priorities, and availability of resources.

Policy Manager A WLAN Management Software feature that allows you to apply a collection of configuration settings known as a *domain policy*, or part of the policy, to one or more WLAN—Security Switch (WSS) switches. With Policy Manager, you can also merge some or all of the configuration changes you make to a single WSS switch into a domain policy. See also *domain policy*.

port address translation See *PAT*.

Power over Ethernet See *PoE*.

pre-master secret A key generated during the handshake process in Transport Layer Security (TLS) protocol negotiations and used to derive a master secret.

preshared key See *PSK*.

PRF Pseudorandom function. A function that produces effectively unpredictable output. A PRF can use multiple iterations of one or more hash algorithms to achieve its output. The Transport Layer Security (TLS) protocol defines a specific PRF for deriving keying material.

Privacy-Enhanced Mail See *PEM*.

private key In cryptography, one of a pair of keys, one public and one private, that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The private key is provided to only the requestor and never shared. The requestor uses the private key to decrypt text that has been encrypted with the public key by someone else. See also *PKI*; *public key*.

PRNG Pseudorandom number generator. An algorithm of predictable behavior that generates a sequence of numbers with little or no discernible order, except for broad statistical patterns.

Protected Extensible Authentication Protocol See *PEAP*.

Protocol Independent Multicast protocol See *PIM*.

pseudorandom function See *PRF*.

pseudorandom number generator See *PRNG*.

PSK Preshared key. The IEEE 802.11 term for a shared secret, also known as a *shared key*. See *shared secret*.

PTK Pairwise transient key. A value derived from a pairwise master key (PMK) and split into multiple encryption keys and message integrity code (MIC) keys for use by a client and server as temporal session keys for IEEE 802.11i robust security. See also *802.11i*.

public key In cryptography, one of a pair of keys, one public and one private, that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The public key is made publicly available for encryption and decryption. See also *PKI*; *private key*.

Public-Key Cryptography Standards See *PKCS*.

public-key infrastructure See *PKI*.

PVST+ Per-VLAN Spanning Tree protocol. A proprietary Cisco protocol that supports a separate instance of the Spanning Tree Protocol (STP) for each virtual LAN (VLAN) in a network and maps the multiple spanning trees to a single tree, to comply with the IEEE 802.1Q specification. See also *STP*.

QoS Quality of service. A networking technology that seeks to measure, improve, and guarantee transmission rates, error rates, and other performance characteristics, based on priorities, policies, and reservation criteria arranged in advance. Some protocols allow packets or streams to include QoS requirements.

quality of service See *QoS*.

RA See *registration authority (RA)*.

radio profile A group of parameters, such as the beacon interval, fragmentation threshold, and security policies, that you configure in common across a set of radios in one or more Access Point (AP) access ports. A few parameters, such as the radio name and channel number, must be set separately for each radio.

RADIUS Remote Authentication Dial-In User Service. A client-server security protocol described in RFC 2865 and RFC 2866. RADIUS extensions, including RADIUS support for the Extensible Authentication Protocol (EAP), are described in RFC 2869. Originally developed by Livingston Enterprises, Inc., to authenticate, authorize, and account for dial-up users, RADIUS has been widely extended to broadband and enterprise networking. The RADIUS server stores user profiles, which include passwords and authorization attributes.

RC4 A common encryption algorithm, designed by RSA Data Security, Inc., used by the Wired-Equivalent Privacy (WEP) protocol and Temporal Key Integrity Protocol (TKIP).

received signal strength indication See *RSSI*.

registration authority (RA) Network software that verifies a user (client) request for a digital certificate and instructs the certificate authority (CA) to issue the certificate. Registration authorities are part of a public-key infrastructure (PKI), which enables secure exchanges of information over a network. The digital certificate contains a public key for encrypting and decrypting messages and digital signatures.

Remote Authentication Dial-In User Service See *RADIUS*.

restricted access Permission to use most WLAN 2300 System Software (WSS Software) command-line interface (CLI) commands required for viewing status information (**show** commands), except those that list security information in clear text. Users with restricted access can clear ARP requests and ping hosts. Compare *enabled access*.

RF detection sweep A comprehensive search for radio frequency (RF) signals within a Mobility Domain™ group, to locate rogue clients, rogue access ports, and ad hoc users. A sweep can be either a scheduled sweep or a continuous *SentrySweep*™ search. During a scheduled sweep, each included Access Point (AP) access point radio sweeps all channels in the IEEE 802.11b/g and 802.11a spectrum. In contrast, SentrySweep operates only on the disabled radios in a Mobility Domain and does not disrupt service.

roaming The ability of a wireless user (client) to maintain network access when moving between access ports (APs).

robust security network See *RSN*.

rogue access port An access point (AP) that is not authorized to operate within a wireless network. Rogue access ports subvert the security of an enterprise network by allowing potentially unchallenged access to the enterprise network by any wireless user (client) in the physical vicinity.

rogue client A user (client) who is not recognized within a network, but who gains access to it by intercepting and modifying transmissions to circumvent the normal authorization and authentication processes.

RSA A public-key algorithm developed in 1977 by RSA Data Security, Inc., used for encryption, digital signatures, and key exchange.

RSN Robust security network. A secure wireless LAN (WLAN) based on the developing IEEE 802.11i standard.

RSSI Received signal strength indication. The received strength of an incoming radio frequency (RF) signal, typically measured in decibels referred to 1 milliwatt (dBm).

scalability The ability to adapt easily to increased or decreased requirements without impairing performance.

secure hashing algorithm See *SHA*.

Secure Shell protocol See *SSH*.

Secure Sockets Layer protocol See *SSL*.

security ACL Security access control list. An ordered list of rules to control access to and from a network by determining whether to forward or filter packets that are entering or exiting it. Associating a security ACL with a particular user, port, virtual LAN (VLAN), or virtual port on a WLAN—Security Switch (WSS) switch controls the network traffic to or from the user, port, VLAN, or virtual port. The rules in an ACL are known as *access control entries (ACEs)*. See also *ACE*.

seed (1) An input to a pseudorandom number generator (PRNG), that is generally the combination of two or more inputs. (2) The WLAN—Security Switch (WSS) switch that distributes information to all the WSS switches in a Mobility Domain™ group.

SentrySweep™ A radio frequency (RF) detection sweep that runs continuously on the disabled radios in a Mobility Domain™ group. See also *RF detection sweep*.

session A related set of communication transactions between an authenticated user (client) and the specific station to which the client is bound.

Session Initialization Protocol See *SIP*.

service set identifier See *SSID*.

SHA Secure hashing algorithm. A one-way hashing algorithm used in many authentication algorithms and also for key derivation in many algorithms. A SHA produces a 160-bit hash.

shared secret A static key distributed by an out-of-band mechanism to both the sender and receiver. Also known as a *shared key* or *preshared key (PSK)*, a shared secret is used as input to a one-way hash algorithm. When a shared secret is used for authentication, if the hash output of both sender and receiver is the same, they share the same secret and are authenticated. A shared secret can also be used for encryption key generation and key derivation.

SIP Session Initialization Protocol. A signaling protocol that establishes real-time calls and conferences over IP networks.

Spanning Tree Protocol See *STP*.

SSH Secure Shell protocol. A Telnet-like protocol that establishes an encrypted session.

SSID Service set identifier. The unique name shared among all computers and other devices in a wireless LAN (WLAN).

SSL Secure Sockets Layer protocol. A protocol developed by Netscape for managing the security of message transmission over the Internet. SSL has been succeeded by Transport Layer Security (TLS) protocol, which is based on SSL. The *sockets* part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA Data Security, Inc., which also includes the use of a digital certificate. See also *HTTPS*; *TLS*.

station Any device with a media access control (MAC) address and a Physical layer (PHY) interface to the wireless medium that comply with the standards for all IEEE 802 networks. Wireless clients and Access Point (AP) access points are stations in a Nortel WLAN 2300 System.

STP Spanning Tree Protocol. A link management protocol, defined in the IEEE 802.1D standard, that provides path redundancy while preventing undesirable loops in a network. STP is also known as *Spanning Tree Bridge Protocol*.

subnet mobility The ability of a wireless user (client) to roam across Access Point (AP) access ports and WLAN—Security Switch (WSS) switches in a virtual LAN (VLAN) while maintaining a single IP address and associated data sessions.

supplicant A client that is attempting to access a network.

syslog server A remote repository for log messages. Nortel WLAN 2300 System Software (WSS Software) supports up to four syslog servers on virtual LANs (VLANs) whose locations are configurable. WSS Software log protocol complies with RFC 3164.

TAPA™ Nortel access point Access™ protocol. A point-to-point datagram protocol, developed by Nortel , that defines the way each Access Point (AP) access point communicates with a WLAN—Security Switch (WSS) switch in a Nortel WLAN 2300 System. By means of TAPA, AP access ports announce their presence to the WSS, accept configuration from it, relay traffic to and from it, announce the arrival and departure of users (clients), and provide statistics to the WSS on command.

Temporal Key Integrity Protocol See *TKIP*.

TKIP Temporal Key Integrity Protocol. A wireless encryption protocol that fixes the known problems in the Wired-Equivalent Privacy (WEP) protocol for existing IEEE 802.11 products. Like WEP, TKIP uses RC4 ciphering, but adds functions such as a 128-bit encryption key, a 48-bit initialization vector, a new message integrity code (MIC), and initialization vector (IV) sequencing rules to provide better protection. See also *802.11i*; *CCMP*.

TLS Transport Layer Security protocol. An authentication and encryption protocol that is the successor to the Secure Sockets Layer (SSL) protocol for private transmission over the Internet. Defined in RFC 2246, TLS provides mutual authentication with nonrepudiation, encryption, algorithm negotiation, secure key derivation, and message integrity checking. TLS has been adapted for use in wireless LANs (WLANs) and is used widely in IEEE 802.1X authentication. See also *EAP-TLS*; *PEAP*; *TTLS*.

TLV Type, length, and value. A methodology for coding parameters within a frame. *Type* indicates a parameter's type, *length* indicates the length of its value, and *value* indicates the parameter's value.

Transport Layer Security protocol See *TLS*.

TTLS Tunneled Transport Layer Security. An Extensible Authentication Protocol (EAP) method developed by Funk Software, Inc., and Certicom for 802.1X authentication. TTLS uses a combination of certificates and password challenge and response for authentication. The entire EAP subprotocol exchange of attribute-value pairs takes place inside an encrypted transport layer security (TLS) tunnel. TTLS supports authentication methods defined by EAP, as well as the older Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), Microsoft CHAP (MS-CHAP), and MS-CHAPV2. Compare *EAP-TLS*; *PEAP*.

Nortel access point Access protocol See *TAPA™*.

Tunneled Transport Layer Security subprotocol See *TTLS*.

tunneling The transmission of data by one network through the connections of another network by encapsulating its data and protocol information within the other network's transmission units. To forward traffic for a roaming user within a Mobility Domain™ group, a WLAN—Security Switch (WSS) switch that is not a member of the user's virtual LAN (VLAN) creates a tunnel to another WSS switch on which the user's VLAN is configured.

type, length, and value See *TLV*.

U-NII Unlicensed National Information Infrastructure. Three unlicensed frequency bands of 100 MHz each in the 5 GHz band, designated by the U.S. Federal Communications Commission (FCC) to provide high-speed wireless networking. The three frequency bands—5.15 GHz through 5.25 GHz (for indoor use only), 5.25 GHz through 5.35 GHz, and 5.725 GHz through 5.825 GHz—were allocated in 1997.

Unlicensed National Information Infrastructure See *U-NII*.

user A person who uses a client. In a Nortel WLAN 2300 System, users are indexed by username and associated with authorization attributes such as user group membership.

user wildcard A Nortel convention for matching fully qualified structured usernames or sets of usernames during authentication by means of known characters plus two special "wildcard" characters. Double asterisks (**) represent *all* usernames. A single asterisk (*) can appear either before or after the delimiter in a user wildcard and can represent any number of characters up to the next delimiter. A delimiter can be an *at* (@) sign or a dot (.). See also *MAC address wildcard*; *VLAN wildcard*.

user group A collection of users with the same authorization attributes.

vendor-specific attribute See *VSA*.

virtual LAN See *VLAN*.

VLAN Virtual LAN. A set of ports that share a single Layer 2 network. Because the ports that constitute a VLAN can be on a single network device or multiple devices, VLANs enable you to partition a physical network into logical networks that meet the needs of your organization. You can divide a single device into multiple logical Layer 2 switches, with each VLAN operating as a separate switch, or make multiple devices members of multiple logical Layer 2 networks. By default, all WLAN—Security Switch (WSS) switch ports are members of VLAN 1, which is named *default*.

VLAN wildcard A Nortel convention for applying the authentication, authorization, and accounting (AAA) attributes in the location policy on an WSS switch to one or more users, based on a virtual LAN (VLAN) attribute. To specify all VLANs, use the double-asterisk (**) wildcard characters. To match any number of characters up to, but not including a delimiter character in the wildcard, use the single-asterisk wildcard. Valid VLAN wildcard delimiter characters are the *at* (@) sign and the dot (.). See also *location policy*; *MAC address wildcard*; *user wildcard*.

Voice over IP See *VoIP*.

VoIP Voice over IP. The ability of an IP network to carry telephone voice signals as IP packets in compliance with International Telecommunications Union Telecommunication Standardization Sector (ITU-T) specification H.323. VoIP enables a router to transmit telephone calls and faxes over the Internet with no loss in functionality, reliability, or voice quality.

VSA Vendor-specific attribute. A type of RADIUS attribute that enables a vendor to extend RADIUS operations to fit its own products, without conflicting with existing RADIUS attributes or the VSAs of other companies. Companies can create new authentication and accounting attributes as VSAs.

watch list A WLAN Management Software method for monitoring user location and activity. After initially finding a user through WLAN Management Software , you can add the user to the watch list for continued monitoring. WLAN Management Software tracks and displays such information as the Access Point (AP) access port(s) that a user is associated with during a session, the server that authenticated the user, and the session start and stop times.

Web View A Web-based application for configuring and managing a single WLAN—Security Switch (WSS) switch and its attached Access Point (AP) access ports through a Web browser. Web View uses a secure connection that implements Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS).

WECA Wireless Ethernet Compatibility Alliance. See *Wi-Fi Alliance*.

WEP Wired-Equivalent Privacy protocol. A security protocol, specified in the IEEE 802.11 standard, that attempts to provide a wireless LAN (WLAN) with a minimal level of security and privacy comparable to a typical wired LAN. WEP encrypts data transmitted over the WLAN to protect the vulnerable wireless connection between users (clients) and access ports (APs). Although appropriate for most home use, WEP is weak and fundamentally flawed for enterprise use. Compare *AES*; *CCMP*; *TKIP*.

Wi-Fi Alliance An organization formed by leading wireless equipment and software providers, for certifying all IEEE 802.11 wireless LAN (WLAN) products for interoperability and promoting the term *Wi-Fi* as their global brand name. Only products that pass Wi-Fi Alliance testing can be certified. Certified products are required to carry an identifying seal on their packaging stating that the product is Wi-Fi certified and indicating the radio frequency band used (2.4 GHz for 802.11b and 5 GHz for 802.11a, for example). The Wi-Fi Alliance was formerly known as the *Wireless Ethernet Compatibility Alliance (WECA)*.

Wi-Fi Protected Access See *WPA*.

wildcard mask A 32-bit quantity used with an IP address to determine which bits in the address to ignore in a comparison with another IP address. When setting up security access control lists (ACLs), you specify source and destination IP addresses and corresponding wildcard masks by which the WSS switch determines whether to forward or filter packets. The security ACL checks the bits in IP addresses that correspond to any *0*s (zeros) in the mask, but does not check the bits that correspond to *1*s (ones) in the mask.

wired authentication port An Ethernet port that has 802.1X authentication enabled for access control.

Wired-Equivalent Privacy protocol See *WEP*.

Wireless Ethernet Compatibility Alliance See *Wi-Fi Alliance*.

wireless Internet service provider See *WISP*.

wireless LAN See *WLAN*.

WISP Wireless Internet service provider. A company that provides public wireless LAN (WLAN) services.

WLAN Wireless LAN. A LAN to which mobile users (clients) can connect and communicate by means of high-frequency radio waves rather than wires. WLANs are defined in the IEEE 802.11 standard.

WLAN Management Software ™ A tool suite for planning, configuring, deploying, and managing a Nortel WLAN 2300 System wireless LAN (WLAN). Based on site and user requirements, WLAN Management Software determines the location of WLAN—Security Switch (WSS) switches and Access Point (AP) access points and can store and verify configuration information before installation. After installation, WLAN Management Software deploys the settings on the equipment and manages and verifies configuration changes. To monitor network performance, WLAN Management Software collects WSS and AP information, calculates and displays AP neighbor relationships, and detects anomalous events—for example, rogue access ports.

WLAN 2300 System Software™ (WSS Software**™)** The Nortel operating system, accessible through a command-line interface (CLI) or the WLAN Management Software tool suite, that enables Nortel WLAN 2300 System products to operate as a single system. WLAN 2300 System Software (WSS Software) performs authentication, authorization, and accounting (AAA) functions; manages WLAN—Security Switch (WSS) switches and Access Point (AP) access ports; and maintains the wireless LAN (WLAN) by means of such network structures as Mobility Domain™ groups, virtual LANs (VLANs), tunnels, spanning trees, and link aggregation.

WPA Wi-Fi Protected Access. The Wi-Fi Alliance's version of the Temporal Key Integrity Protocol (TKIP) that also includes a message integrity code (MIC) known as *Michael*. Although WPA provides greater wireless security than the Wired-Equivalent Privacy protocol (WEP), WPA is not as secure as IEEE 802.11i, which includes both the RC4 encryption used in WEP and Advanced Encryption Standard (AES) encryption, but is not yet ratified by IEEE. See also *AES*; *RC4*; *TKIP*.

WPA IE A set of extra fields in a wireless frame that contain Wi-Fi Protected Access (WPA) information for the access point or client. For example, a Access Point (AP) access point uses the WPA IE in a beacon frame to advertise the cipher suites and authentication methods that the AP access point supports for its encrypted SSID.

WPA information element See *WPA IE*.

WSS See *Wireless Security Switch™ (WSS™)*.

X.500 A standard of the International Organization for Standardization (ISO) and International Telecommunications Union Telecommunication Standardization Sector (ITU-T), for systematically collecting the names of people in an organization into an electronic directory that can be part of a global directory available to anyone in the world with Internet access.

X.509 An International Telecommunications Union Telecommunication Standardization Sector (ITU-T) Recommendation and the most widely used standard for defining digital certificates.

XML Extensible Markup Language. A simpler and easier-to-use subset of the Standard Generalized Markup Language (SGML), with unlimited, self-defining markup symbols (tags). Developed by the World Wide Web Consortium (W3C), the XML specification provides a flexible way to create common information formats and share both the format and the data on the Internet, intranets, and elsewhere. Designers can create their own customized tags to define, transmit, validate, and interpret data between applications and between organizations.

Index

Numerics

802.11a 76, 256, 258
802.11b 76, 256, 258
802.11g 76, 256, 258
802.11i. See RSN
802.1Q tagging 91
802.1X
  authentication 417
  authentication port control 491
  authorization 469
  client reauthentication 496
  clients 503
  configuration display 504
  information 502
  key transmission 492
  order of processing 467
  protocol 415
  quiet period 500
  settings 489
  statistics 505
  timeout 501

A

AAA (authentication, authorization, and accounting)
  administrative access, configuring 51, 54
  configuration scenarios for administrators 66
  configuration, displaying 464
  network users 401
  order of processing 467
  servers, traffic ports for 605
AAA methods 63, 412
access
  administrative, configuring 54
  to console 56
access control entries (ACEs) 353
access control lists. See security ACLs
access controls, in a Mobility Domain 605
access levels, command line 50
Access Point (AP)
  fingerprint 261
Access Point (AP) signatures 549
Access Point. See AP (Access Point)
access points
  rogues 538
  See also AP (Access Point)
Access Points (APs)
  Wi-Fi Multimedia (WMM) 305
accounting 410
  order of processing 467
  supported RADIUS attributes 599
  users 460
accounting records 460
  administrators 63
  local users 462
  roaming users 463
  start-stop 460
  stop-only 460
  updating 460
Acct-Authentic attribute 602
Acct-Delay-Time attribute 601
Acct-Input-Gigawords attribute 603
Acct-Input-Octets attribute 602
Acct-Input-Packets attribute 602
Acct-Multi-Session-Id attribute 602
Acct-Output-Gigawords attribute 603
Acct-Output-Octets attribute 602
Acct-Output-Packets attribute 602
Acct-Session-Id attribute 602
Acct-Session-Time attribute 602
Acct-Status-Type attribute 601

ACEs (access control entries) 353
ACLs (access control lists). See security ACLs
active scan 549
ACTIVE user state, for roaming 187
Address Resolution Protocol. See ARP
ad-hoc networks 555
administrative access 122
  configuring 54
  enabling 57
administrative access mode
  defined 35, 55
  prohibited for MAC users 426
administrative Certificate Signing Request 391
administrators
  accounting 63
  console sessions, clearing 509
  console sessions, displaying 509
  privileges 57
  sessions, clearing 507
  sessions, displaying 507
  Telnet client sessions, displaying and clearing 511
  Telnet sessions, displaying and clearing 510
advisory notices, explanations of 33
affinity 91
  configuring 95
  in roaming VLANs 185
  number 185
aging timeout
  ARP 150
  FDB 102
alert logging level 576
aliases 133
all access 50
antenna, external 258
AP (Access Point)
  boot process 231
  configuration template 251
  configuring 74, 76, 221
  defaults 247
  denial of configuration information, troubleshooting 572
  directly connected compared to distributed 224
  displaying information 281
  Distributed AP, configuring 258
  dual homing 227
  dual homing, configuring 260
  LED blink mode 260
  naming 259
  restarting 281
  security 261
  session load balancing 260
  status 288
  WSS ports 72
  WSS ports, configuring 74, 256
ARP aging timeout 150
ARP entries
  adding 149
  displaying 148
ARP table 147
asterisks. See double asterisks (**); single asterisks (*)
attack list 547
attributes
  assigning to network users 450
  authorization 428
  Encryption-Type 451, 604
  precedence of user over group value 61
  RADIUS. See RADIUS attributes
  reassigning with the location policy 455
authentication
  console, for administrative access 63, 68
  defined 410
  effects on encryption 417
  failure, troubleshooting 573
  local 416
  local backup with remote 413
  local, configuration scenarios 67
  MAC address, to local database 425
  non-802.1X default 478
  offload 416, 418
  order of processing 467
  pass-through 416
  pass-through with local backup 413
  pass-through, configuring 419
  protocols 415
  RADIUS, for Telnet users 68
  remote with local backup 413

security ACLs and 365
server 479
session timeout 502
unresponsive RADIUS servers, scenario 70
via local database 420
wired ports 490
WPA 199
authentication, authorization, and accounting. See AAA (authentication, authorization, and accounting) 51, 54
authenticator, pass-through, WSS as 381
authorization 410, 468
attributes, assigning 450
order of processing 467
port lists 469
server setting for timeouts 501
server timeout 501
authorization attributes
Encryption-Type 451
local database assignment 446
security ACL 451
user group assignment 451
authorization password
MAC 428
outbound 428
authorization server timeout 501
autonegotiation 81
autosensing 81
Avaya voice over IP 376

B

backbone fast convergence 319
configuring 323
beacon interval 268
before editbuffer-index
defined 361
locating an ACE 371
black list 546
blink mode 260
blocked ports, displaying 329
Bonded Auth 421
boot information 520
bridge priority
configuring 315
defined 313
broadcast
DTIM interval 268
preamble length 271
buffer
edit. See edit buffer
history 45
system, for logging 576

C

CA. See certificate authority
Called-Station-Id attribute 601
Calling-Station-Id attribute 601
case in usernames and passwords 62
Catalyst switch, interoperating with load-sharing port groups 88
CCMP 195
enabling 203, 207
certificate authority
certificate source 381
enrolling with 391
Certificate Signing Request (CSR) 387
defined 385
generating 391
certificates
configuration scenarios 393
creating 385
EAP self-signed 389
invalid, troubleshooting 572
overview 379
PKCS #12 object file 387
self-signed 387
supported on the WSS 384
Web 389
Certification Request Syntax Standard 385
channels
channel number, setting 246
configuring 273
CHAP-Password attribute 600
CIDR format for subnet masks in command entries 38
cipher suites, RSN

enabling 207
cipher suites, WPA 195
enabling 203
Class attribute 601
class of service. See CoS (class of service)
classless interdomain routing (CIDR) format 38
clear SSID 241
CLI (command-line interface)
command description format 50
command prompts 36
conventions 35
help 49
history buffer command reuse 45
IP address and mask notation 38
keyboard shortcuts 44
list formats 41
MAC address globs 39
MAC address notation 38
overview 35
port list conventions 41
subnet masks 38
syntax notation 37
tabs for command completion 46
text entry conventions 38
user globs 39
VLAN identification 42
wildcard mask notation 38
client black list 546
clients
802.1X 503
DNS 130
HTTPS 128
no network access, troubleshooting 573
NTP 146
Telnet 126
wireless. See users
WPA 201
command description format 50
command name description 50
command prompts 36
command version history 50
command-line interface. See CLI (command-line interface)
committed security ACLs
deleting 365
mapping 365
viewing 363
community strings 158
computer authentication 421
configuration
displaying 527
loading 531
missing, troubleshooting 573
resetting 532
saving 65, 529
setting 530
configuration file 517
See also configuration
configuration template, APs 251
connection modes, CLI 35
connections
dual-homed 227
port groups 87
verifying 150
console
access 56
authentication 60
disabling log output 579
first-time configuration on 56
logging system messages to 579
no authentication 60
passwords 63
sessions, clearing 509
sessions, displaying 509
target 576
conventions
CLI 35
conventions, text and syntax 34
CoS (class of service)
default 355
filtering by, in security ACLs 354
priority assigned 355
countermeasures 537
enabling 548
SNMP notifications 550
countermeasures, TKIP 198
configuring 204, 208
counters

radio 289
See also statistics
country, specifying 248
critical logging level 576
Cryptographic Message Syntax Standard 385
current TTY session 576

D

database, local
clearing users from 63
mapping security ACLs to users in 451
date, configuring 136
daylight savings time, configuring 138
DEASSOCIATED user state, for roaming 187
debug logging level 577
delimiter characters, for user globs 39
delivery traffic indication map (DTIM) interval 268
Denial-of-Service (DoS) protection 550
destination, logging 576
DHCP client 109
DHCP option 43 225, 232
DHCP server 607
diagnostics 582
digital certificates. See certificates
digital signatures 380
directory, displaying 521
Distributed APs
configuring 221
See also AP (Access Point)
Distributed MPs
mapping security ACLs to 368
DNS (Domain Name Service) 128, 605
client 130
domain name 132
servers 131
servers, displaying 133
documentation conventions 34
documentation, product 32
domain name 132
Domain Name Service. See DNS (Domain Name Service)
DoS attacks 552
dotted decimal notation, in IP addresses 38
double asterisks (**)
in user globs 39
in VLAN globs 40
wildcard 48
draft-congdon-radius-8021x-29.txt 599
DTIM (delivery traffic indication map) interval 268
dual homing 227
configuring 260
dynamic entries
ARP 149
FDB 97
Dynamic Frequency Selection (DFS) 541
dynamic security ACLs. See user-based security ACLs
dynamic tuning 291
dynamic WEP 492

E

EAP (Extensible Authentication Protocol)
authentication, available encryption 417
defined 402, 415
offload 418
pass-through authentication 419
RADIUS authentication 478
self-signed certificate 389
EAP-MD5 authentication protocol 415
EAPoL key messages 492
EAP-TLS authentication protocol 415
edit buffer
displaying 363
temporary storage for security ACLs 353
emergency logging level 576
enable password 58
changing 58
initial settings 57
enabled access 50
configuring 57
enabled mode. See enabled access
encrypted SSID 241
encryption
affects of authentication methods on 417

assigning a type locally 454
assigning a type on a RADIUS server 455
clearing types from users 455
configuration scenarios 212
effects of authentication on 417
radios 191
encryption keys
configuration scenarios 393
overview 379
public and private 383
Encryption-Type attribute 604
assigning 451, 454
End-Date attribute
description 604
enrolling with a certificate authority 391
eq (equal to) operator
in security ACLs 359
in the location policy 458
error logging level 576
EtherChannel interoperability 88
Ethernet ports, numbering conventions 41
Event-Timestamp attribute 603
Extensible Authentication Protocol (EAP). See EAP (Extensible Authentication Protocol)
external antenna 258

F

factory reset switch 574
fallthru authentication type
changing 265
fast convergence features 319
backbone fast convergence 319
backbone fast convergence, configuring 323
port fast convergence 319
port fast convergence, configuring 321
uplink fast convergence 320
uplink fast convergence, configuring 325
FDB (forwarding database) 96
adding entries 100
displaying 99
removing entries 101
timers 102
files
copying 522
deleting 524
directory 521
Filter-Id attribute 600
reassigning with the location policy 455
filters, packet 351
reassigning in a location policy rule 458
fingerprint
Access Point (AP) 261
firewalls, in a Mobility Domain 605
firmware, automatic upgrades 260
first-time configuration, via the console 56
flash memory. See nonvolatile storage
flood attacks 551
forgotten system password 574
forwarding database. See FDB (forwarding database)
forwarding delay
configuring 318
defined 318
fragmentation threshold 269

G

global RADIUS defaults, setting 479
globs. See MAC address globs; user globs; VLAN globs
grace period, for roaming 188
gt (greater than) operator in security ACLs 359
guest users, last-resort access 440

H

hello interval
configuring 318
defined 318
help, command-line 49
history buffer, reusing commands in 45
history, command version 50
hits, security ACLs
configuring 364
sampling 364
HTTPS, disabling 128

I

ICMP ACLs 357
IEEE 802.1X 415
IGMP snooping 335
  displaying information 344
  enabling 335
  last member query interval 336
  last member query interval, configuring 340
  other-querier-present interval 336
  other-querier-present interval, configuring 338
  proxy reporting 335
  pseudo-querier 336
  querier, displaying 347
  query interval 336
  query interval, configuring 337
  query response interval 336
  query response interval, configuring 339
  robustness value 336
  robustness value, configuring 341
  router solicitation 341
  statistics 346
  timers 336
ignore list 548
image file 517
  boot information 520
  upgrading 535
info logging level 577
information element 200
informs, SNMP 162
input filters, reassigning 458
interfering device 538
Internet Control Message Protocol (ICMP) ACLs 357
Internet Group Management Protocol. See IGMP snooping
interval, WEP rekey 494
Intrusion Detection System (IDS) 550
  ad-hoc networks 555
  DoS attacks 552
  flood attacks 551
  log messages 559
  Netstumbler 553
  weak WEP keys 556
  Wellenreiter 553
  wireless bridges 554
invalid certificate, troubleshooting 572
IP ACLs 354
IP addresses
  aliases 133
  configuring 109
  conventions for entry and display 38
  disabling 112
  displaying 114
  removing 113
  subnet masks for, notation conventions 38
  system IP address 114, 115
  verifying 150
  wildcard masks for, in security ACLs 355
IP interfaces, configuration scenario 152
IP phones 376
IP routes 117
  default 121
  displaying 119
  static 121
  tracing 152

K

key pair, public-private 388
key transmission
  enabling and disabling 491
  time intervals 493
keyboard shortcuts for command entry 44
keys
  802.1X WEP rekeying 494
  public-private pair, creating 388
  static WEP 211
  transmission of 802.1X key information 492

L

last member query interval 336
  configuring 340
last-resort authentication
  available encryption 417
last-resort username 440
  passwords are invalid 62, 440
LEDs, AP blink mode 260

list formats for command entry 41
load balancing
  AP access points 260
  RADIUS server groups 484
load-sharing port groups 87
  displaying 88
  EtherChannel interoperability 88
local AAA method 412
local accounting records 462
local authentication
  802.1X, configuring 420
  configuration scenario 67
  console users, scenario 68
  defined 416
  local override and backup authentication, scenario 69
local database 63
  assigning encryption types in 454
  assigning security ACLs in 451
  clearing users from 63
local facility, for log messages sent to a server 580
local override 52, 413
location policy
  compared to a security ACL 457
  configuration scenario 476
  configuring 458
  defined 455
  disabling 460
  displaying rules in 459
  order of rules in 459
location policy rules
  clearing 460
  configuring 458
  defined 456
  displaying 459
  positioning 459
  reassigning security ACLs 458
log configuration 581
log message components 575
logging
  console 579
  current session 580
  displaying current configuration 581
  nonvolatile buffer 578
  session defaults 580
  syslog server 579
  trace, clearing 585
  trace, viewing 584
logging destinations, configuring 576
logging targets, configuring 576
long retry threshold 269
lost system password 574
lt (less than) operator in security ACLs 359

M

MAC address globs
  configuring 427
  conventions for 39
  displaying network sessions by 514
  matching order 40
  single asterisks (*) in 39
  wildcards in 39
  See also MAC addresses
MAC addresses
  authentication by 425
  clearing network sessions by 514
  displaying network sessions by 514
  leading zeros in 38
  notation conventions 38
  PDAs 425
  search timer, for roaming 188
  See also MAC address globs
MAC authentication
  available encryption 417
  configuring 425
MAC authorization password 428
MAC user groups 426
MAC users 426
machine authentication 421
management stations 605
manuals, product 32
mapping security ACLs
  clearing security ACL maps 368
  in the local database 451
  on a RADIUS server 452
  to a user session 366
  to ports, VLANs, or virtual ports 368

masks
subnet, notation conventions 38
wildcard, notation conventions 38, 355
maximum age 318
configuring 318
maximum receive threshold 270
maximum transmit threshold 270
members
adding to server groups 485
in a Mobility Domain 178
methods, AAA 412
Mobility Domain
affinity 91
affinity, configuring 95
clearing members from 183
clearing the configuration 182
configuration display 181
configuration scenario 189
configuration status 181
configuring 176
defined 175
members 178
monitoring roaming users 189
names 177
ports for AAA traffic and management services 605
roaming VLANs in 185
seed 175, 177
status 178
Mobility Profile 468, 469
authorization 468
defined 468
Mobility-Profile attribute
description 604
modify editbuffer-index
defined 361
modifying an ACE 372
monitoring
wireless traffic 588
monitors
port statistics 85
WSS performance 575
MSS CLI. See CLI (command-line interface)
multicast
DTIM interval 268
IGMP snooping 335
IGMP snooping, displaying information 344
preamble length 271
receivers 342, 349
router solicitation 341
routers 342, 348
static router ports 342
static WEP keys 212

N

names
globbing in 39
Mobility Domain 177
See also usernames; VLAN names
NAS-Identifier attribute 601
NAS-IP-Address attribute 600
NAS-Port-Id attribute 603
neq (not equal to) operator
in security ACLs 359
in the location policy 458
NETS (Nortel Enterprise Technical Support)
capturing system information for 596
Netstumbler 553
network access mode
defined 35, 55
MAC address authentication 426
network ports 72
network sessions
clearing by MAC address 514
clearing by session ID 516
clearing by username 513
clearing by VLAN name 515
displaying 511
displaying by MAC address 514
displaying by session ID 516
displaying by username 513
displaying by VLAN name 515
verbose information 512
See also sessions
Network Time Protocol. See NTP (Network Time Protocol)
network users

assigning attributes to 450
authenticating and authorizing 410
configuration scenario 470
defined 401
nonvolatile storage
copying files 522
deleting files 524
listing files 521
Nortel Enterprise Technical Support. See NETS (Nortel Enterprise Technical Support)
Nortel Mobility System 31
notice logging level 576
notification target, SNMP 165
notifications
rogue detection 550
notifications, SNMP 162
NTP (Network Time Protocol) 141
AAA and management ports 605
client 146
displaying information 147
servers 142
update interval 144

O

offload authentication
configuring 418
defined 416
EAP 418
PEAP and MS-CHAP-V2 418
PEAP-MS-CHAP-V2 configuration scenario 474
RADIUS 418
one-time password 390, 397
online help, command line 49
operating system
files 517
upgrading 535
other-querier-present interval 336
configuring 338
OTP 390, 397
outbound authorization password 428
output filters, reassigning 458
override, local, scenario 69
overwriting the system password 574

P

packets
CoS handling 355
denying or permitting with security ACLs 351
pass-through authentication
configuration scenario 472
configuring 419
defined 416
keys and certificates on RADIUS server 381
password
case-sensitive 62
enable, changing 58
enable, setting 58
invalid for last-resort users 62, 440
one-time 390, 397
RADIUS 479
recovery if lost 574
user 62
user in local database 63
PDAs, MAC addresses of 425
PEAP-MS-CHAP-V2
configuration scenario 473
defined 415
See also PEAP-MS-CHAP-V2 offload authentication
PEAP-MS-CHAP-V2 offload authentication
configuration scenario 474
configuring 418
with pass-through, scenario 475
PEM 391
performance issues 586
permanent entries
ARP 149
FDB 97
permitted SSID list 545
permitted vendor list 544
Personal Information Exchange Syntax Standard 385
Per-VLAN Spanning Tree (PVST) 311
ping
AAA and management ports 605

setting ICMP parameters for 357
using 150
PKCS #10 object files 385
PKCS #12 object files 385
certificates, choosing 387
PKCS #7 object files 385
PoE (Power over Ethernet)
configuring 82
displaying 84
port bias, configuring 260
port control 491
port cost 313
configuring 316
displaying 328
port fast convergence 319
configuring 321
port groups 87
displaying 88
EtherChannel interoperability 88
port lists
authorization 469
conventions for 41
port priority 314
configuring 317
port types
clearing 77
configuring 72
defaults 72
resetting 77
ports
administrative state 82
autonegotiation 81
blocked by STP, displaying 329
clearing ACL maps from 453
filtering TCP and UDP packets by 359
HTTP 128
HTTPS 128
interface preference 80
mapping security ACLs to 368
naming 79
PoE 82, 84
port groups 87
resetting 83
speed 81
SSH 124
static multicast router 342
statistics 85
statistics monitor 85
STP port cost 313
STP port cost, configuring 316
STP port cost, displaying 328
STP port priority 314
STP port priority, configuring 317
Telnet 127
types. See port types
VLANs, configuration scenario 102
wired, authentication on 490
Power over Ethernet. See PoE (Power over Ethernet)
preamble length 271
Privacy-Enhanced Mail (PEM) 391
private keys 383
product documentation 32
proxy reporting 335
pseudo-querier 336
public key cryptography 383
Public-Key Cryptography Standards (PKCS) 385
public-key infrastructure 382
public-private key pair
Certificate Signing Request 387
creating 388
self-signed certificate 387
PVST+ (Per-VLAN Spanning Tree) 311

Q

QoS 306
querier
displaying 347
pseudo-querier 336
query interval 336
configuring 337
query response interval 336
configuring 339
quiet period, 802.1X 500

R

radar, MP response to 541

radio profiles 244
  assigning radios 277
  configuring 267
  default profile 245
  disabling radios 279
  displaying 287
  enabling 277
  removing 272
  resetting a parameter 272
radios
  assigning to a radio profile 277
  beacon interval 268
  beaconing SSIDs 265
  channels 246, 273
  counters 289
  denial of configuration information, troubleshooting 572
  disabling 277
  DTIM interval 268
  enabling 277
  encryption 191
  fragmentation threshold 269
  long retry threshold 269
  maximum receive threshold 270
  maximum transmit threshold 270
  preamble length 271
  resetting 280
  RTS threshold 268
  short retry threshold 269
  SSIDs 241, 265
  transmit power 246, 273
RADIUS
  accounting ports 605
  assigning attributes to users 450
  assigning encryption types to user sessions 455
  authentication 605
  authentication scenario 68
  authorization server timeout 501
  clearing security ACL maps from users 453
  displaying server configuration 464
  global defaults 479
  load-balancing servers 484
  mapping security ACLs to user sessions 366, 452
  offload authentication 418
  parameters, setting individually 482
  pass-through authentication, configuration scenario 472
  password 479, 482
  password, global 479, 480
  server configuration 479
  server group configuration 483
  server group, configuration scenario 487
  server groups, displaying 464
  timers 483
  unresponsive RADIUS servers, scenario 70
  usage guidelines 599
RADIUS attributes
  accounting, supported 599
  global attributes, resetting 480
  Nortel specific 603
  RFCs for 599
  standard and extended 599
  value characteristics 599
  VLAN assignment 89
  VSAs 603
RADIUS proxy 441
range operator in security ACLs 359
reauthentication
  802.1X client 496
  interval 498
  number of attempts 497
reauthorization attempts 497
receivers, multicast 349
recovering the system password 574
redundancy
  AP links 227
  port groups 87
rekeying WEP 494
remote monitoring 588
Reply-Message attribute 601
Request-To-Send threshold 268
reset cycle 574
resetting the WSS password 574
restart switch 574
RF Auto-Tuning 291
RF detection 537
RFC 2865, RADIUS 599

RFC 2866, RADIUS accounting 599
RFC 2868, RADIUS tunnels 599
RFC 2869, Acct-Input-Gigawords attribute 603
RFC 2869, RADIUS extensions 599
RFC 3164, syslog servers 575
roaming
  accounting records 463
  affinity 91
  affinity, configuring 95
  monitoring roaming clients 189
  required conditions for 187
  timers in 188
  user sessions 186
  See also Mobility Domain
roaming stations 184
roaming VLANs 185
robustness value 336
  configuring 341
rogue access points
  detecting 538
rogue classification 538
rogue detection 537
  active scan 549
  AP signatures 549
  attack list 547
  classification 538
  client black list 546
  displaying information 561
  feature summary 542
  ignore list 548
  logging 550
  permitted SSID list 545
  permitted vendor list 544
  scans 541
  SNMP notifications 550
rogue detection lists 538
  configuring 543
rolling WEP keys 494
rotating WEP keys 494
router discovery. See router solicitation
router solicitation 341
routers, multicast 348
routes 117
  default 121
  displaying 119
  static 121
  tracing 152
RSA Data Security, Inc. 385
RSN
  overview 207
RTS threshold 268
running configuration
  displaying 527
  saving 529

S

safety notices, explanations of 33
saving the configuration 65, 529
scenarios
  AAA for administrators 66
  AAA for local users 66
  IP interfaces and services 152
  keys and certificates 393
  local authentication 67
  local authentication, console users 68
  local override and backup authentication 69
  location policy 476
  Mobility Domain 189
  overriding VLAN assignment 476
  pass-through with local backup authentication 413
  PEAP-MS-CHAP-V2 configuration 473
  PEAP-MS-CHAP-V2 offload authentication 474
  PEAP-MS-CHAP-V2 with pass-through authentication 475
  port and VLAN configuration 102
  problems in configuration order 467
  RADIUS and server group configuration 487
  RADIUS authentication for Telnet users 68
  RADIUS pass-through authentication configuration 472
  security ACL configuration 377
  STP configuration 332
  unresponsive RADIUS servers 70
Secure Sockets Layer protocol (SSL), management ports 605

security
AP (Access Point) 261
security ACLs
ACEs 353
adding an ACE 370
assigning to user 451
authorization attributes 451
clearing ACLs from the edit buffer 373
clearing maps 368
committed, viewing 363
compared to the location policy 457
configuration scenario 377
deleting 365
displaying details in 363
displaying maps for 368
hits 364
ICMP 357
IP 354
locating ACEs 371
mapping 368
mapping to users 366, 451
modifying 369
operators 359
ordering 361
planning maps 353, 368
ports 368
reassigning in a location policy rule 458
sample hit rate 364
TCP 359
TCP source and destination ports 359
UDP 359
UDP source and destination ports 359
user-based 366
virtual ports 368
VLANs 368
wildcard masks for IP addresses 355
seed, Mobility Domain
configuring 177
defined 175
member configuration 178
self-signed certificates
administrative 389
defined 387
EAP 389
generating 389
Web 389
server groups
adding members 485
contact order 483
deleting 487
displaying 464
load balancing 484
servers
DNS 131
DNS, displaying 133
NTP 142
NTP, displaying 147
RADIUS, configuring 479
RADIUS, displaying 464
syslog 576
service profiles 240
configuring 265
displaying 286
service set identifiers. See SSIDs (service set identifiers)
Service-Type attribute 600
session IDs
clearing network sessions by 516
displaying network sessions by 516
session manager 507
sessions 507
administrative 507, 508
current 576
load balancing 260
mapping security ACLs to 366
network 511
roaming 186
roaming, monitoring 189
statistics 516
target 576
See also network sessions
Session-Timeout attribute 601
severity levels, for system logs 576
short retry threshold 269
Simple Network Management Protocol. See SNMP
Simple Network Time Protocol. See NTP (Network Time Protocol)
single asterisks (*)

in MAC address globs 39
in network session information 511
in user globs 39
in VLAN globs 40
wildcard 47
SNMP
community strings 158
informs 162
notifications, rogue detection 550
trap receiver 165
traps 162
SNMP ports
for get and set operations 605
for traps 605
snooping
wireless traffic 588
snooping. See IGMP snooping
SNTP. See NTP (Network Time Protocol)
software version, displaying 518
Spanning Tree Protocol. See STP (Spanning Tree Protocol)
SpectraLink Voice Priority 376
SSH
enabling 123
port number 124
SSID attribute
description 604
SSID list 545
SSIDs (service set identifiers) 241
beaconing 265
configuring 265
SSL management ports
for Web View 605
for WMS 605
Start-Date attribute
description 604
State attribute 601
static entries
ARP 149
FDB 97
static multicast router ports 342
static routes 121
static security ACLs. See security ACLs
static WEP 191
statistics
802.1X 505
AAA sessions 586
accounting 63, 462
IGMP snooping 346
monitor 85
ports 85
sessions 516
STP 330
STP (Spanning Tree Protocol) 311
backbone fast convergence 319
blocked ports, displaying 329
bridge priority 313
bridge priority, configuring 315
configuration scenario 332
displaying information 327
enabling 312
fast convergence features 319
forwarding delay 318
forwarding delay, configuring 318
hello interval 318
hello interval, configuring 318
maximum age 318
maximum age, configuring 318
port cost 313
port cost, configuring 316
port cost, displaying 328
port fast convergence 319
port priority 314
port priority, configuring 317
statistics 330
timers 318
uplink fast convergence 320
subnet masks, notation conventions 38
summertime period, configuring 138
syntax conventions 34
syntax notation 37
syslog server
local facility mapping 580
logging to 579
See also system logs
system configuration
displaying 527
loading 531

missing, troubleshooting 573
saving 529
setting 530
system image file 517
incomplete load, troubleshooting 573
upgrading 535
system image version 518
system IP address 115
assigning to VLAN 114
required on a Mobility Domain seed 176
system logs
configuring 578
destinations 576
disabling output to the console 579
displaying the configuration of 581
managing 575
message components 575
severity levels 576
system password recovery 574
system time, configuring 136

T

tabs, for command completion 46
tag type 91
target
buffer 576
console 576
server 576
sessions 576
trace 576, 584
TCP ACLs 359
TCP ports
filtering packets by 359
packet filter (security ACL) requirements 359
technical support
capturing system information for 595
Telnet
administrative sessions, displaying and clearing 510
client sessions, displaying and clearing 511
disabling 126
logging to the current session 580
management port 605
port number 127
RADIUS authentication, scenario 68
template
AP configuration 251
TFTP, copying files 522
time intervals for 802.1X key transmission 493
time zone, configuring 137
time, configuring 136
Time-Of-Day attribute
description 604
timeout
802.1X authorization server 501
802.1X session 502
ARP aging 150
timers
802.1X authorization 501
802.1X quiet period 500
802.1X reauthentication 498
802.1X reauthentication, in roaming 188
802.1X session 502
ARP aging timeout 150
beacon interval 268
DTIM interval 268
effect on roaming 188
FDB 102
grace period for roaming 188
IGMP snooping 336
MAC address search 188
NTP update interval 144
RADIUS 483
STP 318
TKIP 195
countermeasures 198, 204, 208
enabling 203, 207
TLS encryption 380
TOS level, filtering packets by 354
trace buffer target 576
traceroute 152
traces
caution about levels 582
clearing 583
copying results to a server 585
enabled, displaying 583
logs of, clearing 585

output, displaying 584
results 584
running 582
traffic monitoring 588
traffic ports, typical, in a Mobility Domain 605
transmit power 246
configuring 273
Transport Layer Security (TLS) encryption 380
trap receiver 165
traps 162
troubleshooting
avoiding unintended AAA processing 467
blinking amber Mgmt LED 573
client authentication failure 573
common WSS setup problems 572
denial of AP configuration 572
incomplete boot load 573
invalid certificate 572
missing configuration 573
MSS debugging via trace 582
MSS logging 575
no network access 573
show commands 586
system trace files for 517
VLAN authorization failure 573
WSS 571
TTY sessions, current, logging system messages to 580
Tunnel-Private-Group-ID attribute 89, 603
tunnels
affinity of an WSS for 91
affinity, changing 95
displaying information about 186
in a Mobility Domain 175, 183
type-of-service (TOS) level, filtering packets by 354

U

UDP ACLs 359
UDP ports
filtering packets by 359
packet filter (security ACL) requirements 359
unauthorized access points 538
unicast, static WEP keys 212
update interval, NTP 144
upgrades, MP firmware 260
uplink fast convergence 320
configuring 325
URL attribute
description 604
user globs
avoiding problems in processing with 467
clearing network sessions by 513
conventions for 39
delimiter characters 39
displaying network sessions by 513
double asterisks (**) in 39
matching order 40
single asterisks (*) in 39
wildcards in 39
See also usernames
user passwords 62
user permissions 451
user sessions. See sessions
user VLANs 89
user-based security ACLs
clearing maps 453
mapping 366
See also security ACLs
User-Name attribute 600
usernames
case-sensitive 62
clearing sessions by 513
displaying network sessions by 513
last-resort 440
See also user globs
User-Password attribute 600
users
802.1X 503
accounting 460
adding to local database 63
authentication and authorization 410
clearing from the local database 63
no network access, troubleshooting 573
security ACLs, assigning 451

V

vendor list 544
Vendor-Specific attribute, 802.1X attribute 601
vendor-specific attributes. See VSAs (vendor-specific attributes)
verbose session output 512
version, displaying 518
virtual LANs. See VLANs (virtual LANs)
virtual ports
  clearing ACL maps from 453
  mapping security ACLs to 368
VLAN globs
  clearing sessions on 515
  conventions for 40
  displaying network sessions by 515
  double asterisks (**) in 40
  matching order 40
  single asterisks (*) in 40
  wildcards in 40
  See also VLANs (virtual LANs)
VLAN ID or name 42
VLAN names
  clearing network sessions by 515
  displaying network sessions by 515
  or number 42
VLAN numbers 42
VLAN-Name attribute 89
  description 604
  reassigning with the location policy 455
VLANs (virtual LANs) 88
  affinity 91
  affinity, configuring 95
  assigning users 89
  authorization failure, troubleshooting 573
  clearing ACL maps from 453
  configuring 92
  disconnected, troubleshooting 573
  displaying 96
  mapping security ACLs to 368
  overriding assignment with the location policy 476
  ports, configuration scenario 102
  removing 93
  roaming, displaying 185
  tagging 91
  user assignment 89
  See also VLAN globs; VLAN ID or name; VLAN names; VLAN-Name attribute
voice over IP 376
  Wi-Fi Multimedia (WMM) 305
voice packets, CoS handling for 307
VSAs (vendor-specific attributes)
  Encryption-Type 451, 604
  End-Date 604
  Mobility-Profile 604
  SSID 604
  Start-Date 604
  supported 603
  Time-Of-Day 604
  URL 604
  VLAN-Name 89, 604

W

warning logging level 576
weak WEP keys 556
Web AAA
  self-signed certificate 389
Web View
  access, defined 56
  keys and certificates requirement 379
WebAAA
  configuring 433
  self-signed certificate 389
Wellenreiter 553
WEP (Wired-Equivalent Privacy)
  configuring 209
  disabling rekeying for 494
  dynamic 492
  rekeying broadcast and multicast keys 494
  secret key 494
  static 191
  using with RSN 207
  using with WPA 203
WEP 802.1X keys
  rekey interval 494
  rekeying 494

Wi-Fi Multimedia (WMM) 305
Wi-Fi Protected Access. See WPA (Wi-Fi Protected Access)
wildcard masks 355
  notation conventions 38
wildcards
  in MAC address globs 39
  in user globs 39
  in VLAN globs 40
  masks for in security ACLs 355
wired authentication ports 72
  802.1X settings 489
  configuring 76
Wired-Equivalent Privacy. See WEP (Wired-Equivalent Privacy)
wireless bridges 554
Wireless LAN Security Switch. See WSS (WLAN Security Switch)
wireless session encryption 381
WLAN System Software CLI. See CLI (command-line interface)
WMM 305
WMS
  keys and certificates requirement 379
WMS Enable Password 58
WPA (Wi-Fi Protected Access)
  authentication methods 199
  cipher suites 195
  clients 201
  configuration scenarios 212
  configuring 203
  information element 200
  overview 194
WPA2
  authentication methods 199
  cipher suites 195
  clients 201
  configuring 203
  information element 200
  overview
WPA2. See RSN
WSS (WLAN Security Switch)
  fixing common setup problems 572
  monitoring performance 575
  password recovery 574
  ports. See WSS ports
  troubleshooting 571
WSS ports
  AP access 72
  network 72
  wired authentication 72, 76

X

X.509 digital certificates 384

Command Index

B

backup system 532
boot OPT+=default 574

C

clear {ap | dap} radio 280
clear boot config 532
clear dap 78, 259
clear dot1x bonded-period 423
clear dot1x max-req 495
clear dot1x port-control 491
clear dot1x quiet-period 500
clear dot1x reauth-max 497
clear dot1x reauth-period 498
clear dot1x timeout auth-server 501
clear dot1x timeout supplicant 502
clear dot1x tx-period 493
clear fdb 101
clear igmp statistics 346
clear interface 113
clear ip alias 135
clear ip dns domain 132
clear ip dns server 131
clear ip route 122
clear ip telnet 127
clear location policy 460
clear log 585
clear log buffer 578, 579
clear log server 578, 580
clear log trace 578
clear mac-user 426
clear mac-user attr 427
clear mac-user attr filter-id 453, 455
clear mac-user group 426
clear mac-usergroup 426
clear mac-usergroup attr filter-id 453, 455
clear mobility-domain 182
clear mobility-domain member 183
clear mobility-profile 469
clear ntp server 143
clear ntp update-interval 145
clear port counters 85
clear port name 79
clear port preference 80
clear port type 77, 259
clear port-group 88
clear radio-profile 272
clear radio-profile countermeasures 549
clear radius deadtime 480
clear radius key 480
clear radius retransmit 480
clear radius server 483
clear radius timeout 480
clear rfdetect attack-list 547
clear rfdetect black-list 546
clear rfdetect ssid-list 545
clear rfdetect vendor-list 544
clear rfdevice ignore 548
clear security acl 365
clear security acl map 369
clear server group 485, 487
clear sessions 507
clear sessions admin 508
clear sessions admin ssh 125
clear sessions admin telnet 127
clear sessions console 509
clear sessions network mac-addr 514
clear sessions network session-id 516
clear sessions network user 513
clear sessions network vlan 515, 516
clear sessions session-id 513
clear sessions telnet 151, 510
clear sessions telnet client 511
clear snmp community 158
clear snmp notify target 165
clear snmp profile 162
clear snmp usm 159
clear snoop 591
clear snoop map 592
clear spantree portcost 316
clear spantree portpri 317
clear spantree portvlancost 316
clear spantree portvlanpri 317

clear spantree statistics 332
clear summertime 138
clear system ip-address 117
clear timezone 137
clear trace 583
clear user 63
clear user attr filter-id 453, 455
clear usergroup attr filter-id 453, 455
clear vlan 93
commit security acl 362
copy 522
crypto ca-certificate 392
crypto certificate 391
crypto generate key 388
crypto generate key ssh 123
crypto generate request 391
crypto generate self-signed 389
crypto otp 390, 397
crypto pkcs12 390, 397

D

delete 524
dir 521

E

enable 57

H

hit-sample-rate 364

L

load config 65, 531

M

mkdir 525
monitor port counters 86

P

ping 150, 479

R

reset {ap | dap} 281
reset port 83
restore system 532
rmdir 526

S

save 581
save config 65, 378, 529
save trace 581
set {ap | dap} bias 260
set {ap | dap} blink 260
set {ap | dap} name 260
set {ap | dap} radio antennatype 274
set {ap | dap} radio auto-tune max-power 298
set {ap | dap} radio auto-tune
max-retransmissions 299
set {ap | dap} radio auto-tune min-client-rate 300
set {ap | dap} radio channel 273
set {ap | dap} radio mode 278
set {ap | dap} radio radio-profile 277
set {ap | dap} radio tx-power 273
set {ap | dap} upgrade-firmware 260
set accounting admin 63
set accounting dot1X 460
set ap radio radio-profile 206, 209
set arp 149
set arp agingtime 150
set authentication console 60
set authentication dot1x 417
set authentication dot1x local 420
set authentication mac 427
set authentication proxy 444
set boot configuration-file 530
set dap 76, 258
set dap auto 252
set dap auto bias 254
set dap auto blink 254
set dap auto group 254
set dap auto mode 254
set dap auto persistent 255
set dap auto radio auto-tune auto-tune

min-client-rate 254
set dap auto radio auto-tune max-power 254
set dap auto radio auto-tune
max-retransmissions 254
set dap auto radio mode 254
set dap auto radio radio-profile 254
set dap auto radiotype 254
set dap auto upgrade-firmware 254
set dap fingerprint 263
set dap security 263
set dot1x authcontrol 490
set dot1x bonded-period 423
set dot1x key-tx 492
set dot1x max-req 495
set dot1x port-control 491
set dot1x quiet-period 500
set dot1x reauth 496
set dot1x reauth-max 497
set dot1x reauth-period 498
set dot1x timeout auth-server 501
set dot1x timeout supplicant 502
set dot1x tx-period 493
set dot1x wep-rekey disable 494
set dot1x wep-rekey enable 494
set dot1x wep-rekey-period 494
set enablepass 58, 574
set fdb 100
set fdb agingtime 102
set igmp 335
set igmp lmqi 340
set igmp mrouter 343
set igmp mrsol 341
set igmp mrsol mrsi 342
set igmp oqi 338
set igmp proxy-report 336
set igmp qi 337
set igmp qri 339
set igmp querier 336
set igmp receiver 344
set igmp rv 341
set interface 109
set interface dhcp-server 608
set interface status 112
set ip alias 134
set ip dns 130
set ip dns domain 132
set ip dns server 131
set ip https server 128
set ip route 121
set ip snmp server 167
set ip ssh 124
set ip ssh absolute-timeout 125
set ip ssh idle-timeout 125
set ip ssh server 123
set ip telnet 127
set ip telnet server 126
set location policy 458
set log 578
set log buffer disable 579
set log buffer severity 578
set log console 579
set log console enable 579
set log current disable 581
set log current enable 580
set log current severity 580
set log server 578, 579
set log server disable 580
set log sessions 580
set log sessions disable 580
set log trace 581
set log trace disable 581
set mac-user 426
set mac-user attr encryption-type 454
set mac-user attr filter-id 366, 451
set mac-user group 426
set mac-usergroup attr 426
set mac-usergroup attr encryption-type 454
set mac-usergroup attr filter-id 451
set mobility-domain member 178
set mobility-domain mode member seed-ip 179
set mobility-domain mode seed 177
set mobility-domain mode seed domain-name 177
set mobility-profile 468
set mobility-profile mode enable 469
set ntp 146
set ntp server 142
set ntp update-interval 144
set port 82

set port name 79
set port negotiation 81
set port poe 83
set port preference 80
set port speed 81
set port type ap 74, 257
set port type wired-auth 76
set port-group 87
set radio-profile 267
set radio-profile active-scan 549
set radio-profile auto-tune channel-config 297
set radio-profile auto-tune channel-holddown 297
set radio-profile auto-tune channel-interval 297
set radio-profile auto-tune
power-backoff-timer 298
set radio-profile auto-tune power-config 298
set radio-profile auto-tune power-interval 298
set radio-profile beacon-interval 268, 271
set radio-profile countermeasures 549
set radio-profile dtim-interval 268
set radio-profile frag-threshold 269
set radio-profile long-retry 269
set radio-profile max-rx-lifetime 270
set radio-profile max-tx-lifetime 270
set radio-profile mode 279
set radio-profile preamble-length 271
set radio-profile rts-threshold 269
set radio-profile service-profile 206, 209, 276
set radio-profile short-retry 269
set radio-profile wmm 308
set radius 480
set radius proxy client 444
set radius proxy port 444
set radius server 482
set radius server address key 482
set radius server author-password 428
set rfdetect attack-list 547
set rfdetect black-list 546
set rfdetect signature 549
set rfdetect ssid-list 545
set rfdetect vendor-list 544
set rfdevice ignore 548
set rfdevice log 550
set security acl ip 354, 357
set security acl ip before 371
set security acl ip tcp 359
set security acl map 368
set security acl modify 372
set security acl udp 359
set server group 484
set server group load-balance 485
set server group members 485
set service-profile 203, 207
set service-profile auth-dot1x 205
set service-profile auth-fallthru 265
set service-profile auth-psk 205
set service-profile beaconed 265
set service-profile cipher-ccmp 204, 208
set service-profile cipher-tkip 204, 208
set service-profile cipher-wep104 204, 208
set service-profile cipher-wep40 204, 208
set service-profile psk-phrase 205
set service-profile psk-raw 205
set service-profile rsn-ie 207
set service-profile ssid-name 265
set service-profile ssid-type 265
set service-profile tkip-mc-time 204
set service-profile wep active-multicast-index 212
set service-profile wep active-unicast-index 212
set service-profile wep key-index 211
set service-profile wpa-ie 203
set snmp community 158
set snmp notify target 165
set snmp profile 162
set snmp protocol 157
set snmp security 161
set snmp usm 159
set snoop 590
set snoop map 591
set snoop mode 592
set spantree 312
set spantree backbonefast 323
set spantree fwddelay 318
set spantree hello 318
set spantree maxage 318
set spantree portcost 316
set spantree portfast 321
set spantree portpri 317

set spantree portvlancost 316
set spantree portvlanpri 317
set spantree priority 315
set spantree uplinkfast 325
set summertime 138
set system contact 156
set system countrycode 248
set system ip-address 115
set system location 156
set timedate 139
set timezone 137
set trace 582, 585
set trace authorization 583
set trace sm 582
set user 60, 63, 124, 126
set user attr encryption-type 454
set user attr filter-id 366, 451
set user last-resort password 440
set user password 63, 124, 126
set usergroup attr encryption-type 454
set usergroup attr filter-id 451
set vlan name 92
set vlan port 92
set vlan tunnel-affinity 95
show {ap | dap} config 282
show {ap | dap} counters 289
show {ap | dap} status 288
show aaa 464, 487, 586
show accounting statistics 64, 462
show arp 148
show auto-tune neighbors 302, 303
show boot 520
show config 527
show crypto ca-certificate 393
show crypto certificate 393
show crypto key ssh 124
show dap config auto 252
show dap connection 285
show dap global 283
show dap qos-stats 309
show dap status auto 254
show dap unconfigured 284
show dhcp-server 609
show dot1x 502
show dot1x clients 503
show dot1x config 504
show dot1x stats 505
show fdb 99
show fdb agingtime 102
show fdb count 99
show igmp 345
show igmp mrouter 348
show igmp querier 347
show igmp receiver-table 349
show igmp statistics 346
show interface 114, 586
show ip alias 136
show ip dns 133
show ip https 128
show ip route 119
show ip telnet 126
show location policy 459
show log buffer 578
show log config 581
show log trace 584
show mobility-domain config 181
show mobility-domain status 180
show mobility-profile 469
show ntp 147
show port counters 85
show port poe 84
show port preference 80
show port status 84
show port-group 88
show radio-profile 287
show rfdetect attack-list 547
show rfdetect black-list 546
show rfdetect clients 563
show rfdetect countermeasures 569
show rfdetect counters 564
show rfdetect data 567
show rfdetect mobility-domain 565
show rfdetect ssid-list 545
show rfdetect vendor-list 544
show rfdetect visible 568
show roaming station 184
show roaming vlan 185, 190
show security acl 363, 368

show security acl editbuffer 363
show security acl hits 364
show security acl info 363
show security acl map 368, 369
show service-profile 206, 208, 286
show sessions admin 125, 127, 508
show sessions console 509
show sessions network 511
show sessions network mac-addr 514
show sessions network session-id 516
show sessions network user 513
show sessions network verbose 512
show sessions network vlan 515
show sessions telnet 510
show sessions telnet client 151, 511
show snmp community 169
show snmp counters 173
show snmp notification target 172
show snmp notify profile 171
show snmp status 168
show snmp usm 170
show snoop 592
show snoop info 591
show snoop map 592
show snoop stats 594
show spantree 327
show spantree backbonefast 324
show spantree blockedports 329
show spantree portfast 322
show spantree portvlancost 328
show spantree statistics 330
show spantree uplinkfast 326
show summertime 138
show system 116, 249
show timedate 140
show timezone 137
show trace 583
show tunnel 186, 190
show version 518
show vlan config 96

T

telnet 151
traceroute 152